Centro Universitário Nossa Senhora do Patrocínio

ESTUDO DOS GOLPES NA INTERNET E PROPOSTA DE PLATAFORMA ONLINE DE CAMPANHA DE CONSCIENTIZAÇÃO

Centro Universitário Nossa Senhora do Patrocínio

ESTUDO DOS GOLPES NA INTERNET E PROPOSTA DE PLATAFORMA ONLINE DE CAMPANHA DE CONSCIENTIZAÇÃO

Marcus Vinícius Fogaça dos Santos
Vinícius Aniceto Escano

Salto – SP
2024

ESTUDO DOS GOLPES NA INTERNET E PROPOSTA DE PLATAFORMA ONLINE DE CAMPANHA DE CONSCIENTIZAÇÃO

Projeto apresentado como requisito básico para a apresentação do Trabalho de Graduação Interdisciplinar do Curso de Ciência da Computação

Orientador (a): Davi Fontebasso Marques de Almeida

Salto-SP
2024

SUMÁRIO

ÍNDICE DE FIGURAS

1. INTRODUÇÃO

Nos últimos anos, a crescente integração da internet em todas as esferas da vida humana trouxe consigo inúmeras oportunidades e benefícios, mas também desafios significativos. Um desses desafios é a proliferação de golpes e fraudes online, como traz a matéria “Golpes digitais aumentaram até 35% em 2023 no Brasil”. (Dino, O Globo, 2024) e que segue uma crescente tendência desde 2022 como mostrado nas reportagens “Tentativas de golpes por meios digitais cresceram 20% no segundo trimestre deste ano no Brasil” (Flávia Jannuzzi e Flávia Jácomo, Bom Dia Brasil, 2022) e “Brasileiros sofrem 208 golpes por hora; alta é de 37,9%” (Fabiola Perez, Uol, 2023).

Neste contexto, torna-se imperativo compreender a natureza e as dinâmicas dos golpes na internet, bem como desenvolver estratégias eficazes para prevenção e conscientização. Este estudo propõe-se a investigar os diferentes tipos de golpes praticados online, desde *phishing* e esquemas de pirâmide até falsas ofertas de emprego e fraudes em compras online. Além disso, busca-se compreender as técnicas utilizadas pelos golpistas, as motivações por trás de seus atos e os impactos dessas práticas na sociedade e na economia digital. Além da análise dos golpes em si, este estudo apresenta uma proposta inovadora: o desenvolvimento de uma plataforma online de campanha de conscientização. Esta plataforma terá como objetivo fornecer informações educativas sobre os diferentes tipos de golpes na internet, dicas práticas de segurança cibernética e recursos para ajudar as pessoas a reconhecer e evitar situações de risco online. Além disso, a plataforma incentivará a denúncia de golpes, promover a colaboração entre usuários e autoridades competentes e fornece um espaço para compartilhamento de experiências e apoio mútuo entre as vítimas.

Desta forma, este estudo não apenas contribuirá para uma compreensão mais aprofundada dos golpes na internet e de suas implicações, mas também oferecerá uma ferramenta prática e acessível para ajudar a proteger os usuários contra essas ameaças digitais. Ao promover a conscientização e a educação em segurança cibernética, esperamos contribuir para um ambiente online mais seguro e confiável para todos os usuários.

2. JUSTIFICATIVA

Este trabalho propõe-se a investigar a natureza dos golpes na internet, compreendendo suas estratégias, motivações e impactos. A partir de uma análise abrangente, serão identificados os tipos mais comuns de golpes, tais como phishing, fraudes em compras online, esquemas de pirâmide, entre outros, assim como as vulnerabilidades que tornam os usuários suscetíveis a essas práticas maliciosas.

Além da análise dos golpes em si, este estudo busca desenvolver uma campanha de conscientização eficaz, direcionada tanto aos usuários comuns da internet quanto a organizações e instituições. A ideia é utilizar-se dos mesmos artifícios usados pelos golpistas, sejam mensagens, ligações, e-mails e afins para chamar a atenção do usuário e assim ser redirecionado pra uma plataforma digital a qual será disseminada informações e promoção de boas práticas de segurança na internet, pretende-se capacitar os usuários a identificar e evitar possíveis golpes, contribuindo assim para a redução da incidência desses crimes virtuais e para a proteção da comunidade online. Outra análise será de captar o número de usuários que acessaram a plataforma e quais foram os recursos e meios mais utilizados, a fim de expor a maior fragilidade.

Portanto, este trabalho se justifica pela relevância e urgência de se compreender e combater os golpes na internet para ir de encontro contra a crescente tendencia citada na introdução deste trabalho com as matérias jornalísticas apresentadas, visando não apenas mitigar os prejuízos individuais e coletivos, mas também promover uma cultura de segurança digital e responsabilidade online.

3. OBJETIVOS

3.1 GERAL

Investigar os diferentes tipos de golpes praticados na internet, compreendendo suas técnicas, motivações e impactos, a fim de fornecer uma análise abrangente sobre esse fenômeno e coletar recursos para a elaboração de estratégias eficazes de prevenção e combate aos crimes virtuais.

3.2 ESPECÍFICOS

- Proposto a análise de dados que proveem de pesquisas, reportagens, relatos e afins para identificar os principais pontos de ataque e efetividade de golpes na internet;
- Criar uma plataforma online que servirá de base de conhecimento e como campanha de conscientização destinado a população no geral;
- Desenvolver um sistema de monitoramento que utilize *QR codes* para rastreamento de dados;
- Avaliar a precisão e a eficiência do sistema na identificação de vazamentos de dados;
- Analisar a capacidade do sistema desenvolvido em termos de rapidez e facilidade de implementação;
- Identificar possíveis falhas e limitações do uso de *QR codes* para captura de dados.

4. METODOLOGIA DA PESQUISA

4.1 TIPO DE PESQUISA

Pesquisa Quantitativa: Esta metodologia envolve a coleta e análise de dados numéricos para quantificar fenômenos, como a incidência de diferentes tipos de golpes, perfil das vítimas, impactos econômicos, entre outros. Será realizada por meio de pesquisas online, análise de dados estatísticos de órgãos governamentais, institutos de pesquisa ou empresas especializadas.

Pesquisa Qualitativa: Utilizada para compreender fenômenos sociais mais complexos, a pesquisa qualitativa ajuda a explorar as percepções, experiências e motivações das vítimas de golpes, bem como a dinâmica dos golpistas. Estudar casos, padrões de abordagem e engenharia social agregam valor a esse tipo.

4.2 UNIVERSO E AMOSTRA

Como amostra em um primeiro momento será utilizado dados de organizações governamentais e não governamentais para o levantamento de público que será abordado. Com a criação da plataforma será lançado mil mensagens e e-mails, além da exposição de cartazes com *QR Codes* para induzir o usuário a acessar a plataforma de conscientização em vez de um golpe real.

4.3 MÉTODO DE ANÁLISE

Análise Estatística: Se a pesquisa envolve dados quantitativos, técnicas estatísticas podem ser aplicadas para identificar padrões, correlações e tendências nos dados. Isso pode incluir análise descritiva para resumir os dados, testes de hipóteses para avaliar relações entre variáveis e modelagem estatística para prever comportamentos ou resultados.

Análise de Rede: Se a pesquisa envolve o estudo de interações entre indivíduos ou entidades, a análise de rede pode ser útil para mapear e visualizar essas relações. Isso pode incluir a identificação de atores-chave, comunidades ou grupos de interesse, a análise da centralidade dos nós na rede e a detecção de padrões de conexão.

Análise Comparativa: Esta abordagem envolve a comparação sistemática de diferentes grupos, contextos ou períodos para identificar semelhanças, diferenças ou padrões de variação. Pode ser útil para avaliar a eficácia de diferentes estratégias de conscientização, a prevalência de golpes em diferentes populações ou regiões, ou a evolução dos padrões de golpes ao longo do tempo.

5. PESQUISA E DESENVOLVIMENTO

No ano de 2023, pelo menos 80 mil pessoas foram vítimas de golpes online segundo estudo feito pelas empresas AllowMe, icarros Itaú, OLX, Unico, Who e Zoop apresentado na reportagem “No Brasil, 80 mil pessoas já foram vítimas de golpes online em 2023” (*ecommerce* Brasil, 2023), fora aqueles em que não são registrados pelos órgãos competentes. A reportagem também traz que um tipo de abordagem comum é o golpe de falso pagamento, geralmente por um boleto copiando instituições públicas e privadas para passar veracidade, seguido por invasão de contas o qual o usuário é induzido a fornecer os dados de acesso de redes sociais, contas bancárias e etc., e por fim anúncios falsos para a vítima oferecendo benefícios.

Já o Cointelegraph cita que em 2022, segunda pesquisa da Fortinet, ocorreram cerca de 103 bilhões de tentativas de golpe no Brasil, sendo o segundo no ranking ficando atrás do México.

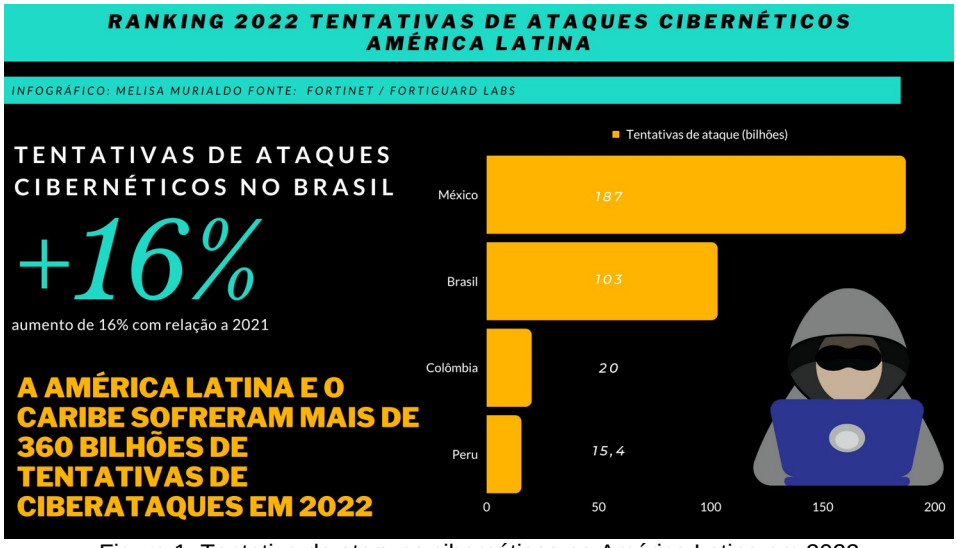

Figura 1: Tentativa de ataques cibernéticos na América Latina em 2022

Também em 2022 um levantamento feito pelo sistema *anti-phishing* da Kapersky relatou cerca de 500 bilhões de tentativas de acessa de links fraudulentos pelo WhatsApp globalmente, desses, 10% são somente no Brasil. Já em 2023 a mesma também registrou cerca de 2,3 milhões de ataques em toda a América Latina.

Uma informação interessante é sobre o app *Cerberus*, que é um aplicativo de rastreamento e considerado um *stalkerware*, de acordo com o gráfico abaixo, o Brasil fica em segundo lugar no ranking de aparelhos com esse aplicativo instalado.

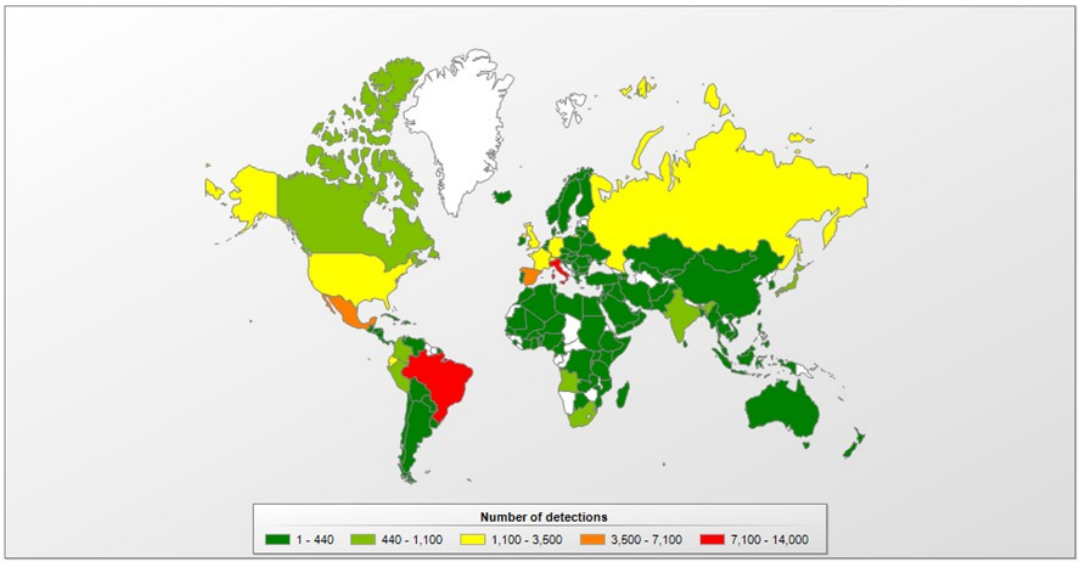

Figura 2: Número de detecções de uso do app Cerberus / Fonte: Kapersky

Outro grande problema crescente no Brasil são os golpes de fraude de identidade, onde os dados da vítima são usados geralmente para acessar serviços financeiros e redes sociais assim realizando operações com dinheiro ou se fazendo passar pela pessoa para pedir a amigos e familiares alguma coisa ou até mesmo ameaçar e causar danos à imagem da vítima. No gráfico abaixo são informados os números no ano de 2022.

TENTATIVAS DE FRAUDE DE IDENTIDADE

2022

Infográfico: Analista Melisa Murialdo Fonte: Serasa Experian

Estado	Tentativas de Fraudes de Identidade 2022	Participação no Total	Variação anual
TOTAL BRASIL	3.879.869		-7,3%
SP	1.191.275	30,7%	-6,8%
RJ	416.839	10,7%	-8,6%
MG	337.386	8,7%	-6,8%
PR	258.991	6,7%	-6,5%
RS	194.360	5%	-6,3%
BA	175.678	4,5%	-8,4%
SC	158.057	4,1%	-5,6%
PE	129.015	3,3%	-8%
GO	117.774	3%	-7,9%
CE	110.673	2,9%	-8,4%
DF	96.585	2,5%	-8,3%
PA	93.282	2,4%	-7,7%
MT	76.962	2%	-5,6%
ES	76.259	2%	-7,3%
MA	61.691	1,6%	-8,9%
AM	59.803	1,5%	-7,6%
MS	55.728	1,4%	-7%
RN	47.084	1,2%	-8,3%
PB	43.571	1,1%	-7,8%
AL	43.569	1,1%	-7,8%
RO	33.238	0,9%	-5,5%
PI	29.812	0,8%	-8,3%
SE	26.314	0,7%	-7,9%
TO	17.417	0,4%	-7,6%
AC	10.627	0,3%	-9,6%
AP	10.497	0,3%	-8,7%
RR	7.382	0,2%	-8,9%

Figura 3: Tentativas de fraude de identidade em 2022

Além da população no geral, instituições públicas e privados também sofrem ataques diariamente e com maior intensidade já que as informações que podem ser adquiridas dessas instituições podem ser sigilosas como segredos de mercado e estratégias ou até mesmo dados sensíveis de operações de empresas e outras entidades. Segundo uma pesquisa feita pela *Check Point* apresentado na reportagem "*Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most" (Check Point, 2023)*, demonstra que cerca de 1248 ataques são realizados por semana para cada empresa no mundo, porém a grande maioria não é bem-sucedida já que as empresas possuem mais recursos e podem criar esquemas de segurança mais eficazes que impede a ação de criminosos.

5.1 **GOLPES NA INTERNET**

Os golpes na internet, também são conhecidos como fraudes online ou cibercrimes. Eles podem assumir diversas abordagens e afetar pessoas, empresas e até mesmo governos.

- ***Phishing*:** Este é um dos golpes mais comuns na internet. Consiste em enviar e-mails fraudulentos que se passam por entidades legítimas, como bancos, empresas ou serviços online populares, na tentativa de obter informações pessoais dos usuários, como senhas, números de cartão de crédito e dados bancários. Os links contidos nesses e-mails geralmente direcionam as vítimas para sites falsos que se parecem muito com os sites originais.
- ***Ransomware*:** Trata-se de um tipo de *malware* que criptografa os arquivos do computador da vítima, tornando-os inacessíveis, e exige um pagamento de resgate (geralmente em criptomoedas) para fornecer a chave de descriptografia. Esse tipo de golpe pode causar danos significativos a empresas e indivíduos, resultando na perda de dados importantes ou até mesmo na paralisação de operações comerciais.
- ***Scams* em redes sociais:** Com o aumento do uso de redes sociais, os golpistas encontraram novas maneiras de se infiltrar e enganar os usuários. Isso pode incluir perfis falsos que se fazem passar por amigos ou conhecidos, oferecendo oportunidades falsas de investimento, vendendo produtos inexistentes ou promovendo esquemas de pirâmide.
- **Falsificação de identidade:** Os golpistas podem roubar informações pessoais de indivíduos através de várias técnicas, como *hacking* de contas online, roubo de documentos físicos ou engenharia social. Com essas informações, podem abrir contas bancárias falsas, fazer compras fraudulentas ou até mesmo cometer crimes em nome da vítima.
- **Golpes de amor/romance:** Este é um tipo de fraude emocional em que os golpistas criam perfis falsos em sites de namoro ou redes sociais, geralmente fingindo ser alguém em quem a vítima pode confiar e desenvolver sentimentos. Eventualmente, eles pedem dinheiro para emergências fictícias ou para facilitar um encontro pessoal, desaparecendo assim que conseguem o que querem.

- **Golpes de investimento:** Com o aumento do interesse em investimentos, especialmente em cripto moedas, os golpistas criaram esquemas fraudulentos de investimento que prometem retornos absurdamente altos em pouco tempo. Muitas vezes, esses esquemas são disfarçados de oportunidades legítimas de investimento, levando as vítimas a perderem grandes quantias de dinheiro.

5.2 TIPOS COMUNS DE GOLPES

5.2.1 *PHISHING*

Os golpes de *phishing* representam uma das formas mais comuns e perigosas de ataques cibernéticos nos dias de hoje, como citado em matéria pela Kapersky, e que realizou a pesquisa menciona “as tentativas de golpe de *phishing* e de trojans bancários tiveram um aumento de 617% e de 50%, respectivamente” analisando os períodos de junho de 2022 até julho de 2023 e junho de 2021 a julho de 2022. Eles envolvem a tentativa de enganar os usuários da internet, geralmente por meio de e-mails, mensagens de texto ou telefonemas, para que revelem informações pessoais, como senhas, números de cartão de crédito, ou cliquem em links maliciosos. Algumas das abordagens são:

- **Engenharia Social:** O *phishing* explora a engenharia social, que é a manipulação psicológica das pessoas para que elas realizem ações específicas. Os golpistas criam mensagens convincentes e persuasivas, muitas vezes se passando por empresas ou instituições legítimas, para induzir as vítimas a revelarem informações confidenciais.
- **E-mails e Mensagens Falsas:** Os e-mails de *phishing* geralmente apresentam sinais de alerta, como erros gramaticais, endereços de e-mail suspeitos ou URLs encurtadas. No entanto, alguns são elaborados com tanta habilidade que podem ser difíceis de detectar, especialmente para usuários menos experientes.
- **Sites Falsos:** Os golpistas muitas vezes criam sites falsos que imitam perfeitamente os sites legítimos de instituições financeiras, empresas de comércio eletrônico, redes sociais e outros serviços populares. Eles usam

esses sites para coletar informações confidenciais quando as vítimas tentam fazer login ou realizar transações.

5.2.2 GOLPES DE INVESTIMENTOS

Os golpes de investimento são esquemas fraudulentos projetados para enganar investidores, muitas vezes prometendo retornos financeiros irrealisticamente altos ou garantidos. Esses golpes exploram a ganância, a falta de conhecimento financeiro e a confiança das pessoas, levando-as a investir em esquemas ilegítimos.

- **Promessas Irreais de Retorno:** Um dos sinais mais comuns de um golpe de investimento é a promessa de retornos financeiros extraordinariamente altos em um curto período de tempo, muitas vezes sem risco. Essas promessas são geralmente muito boas para serem verdadeiras e devem ser vistas com grande ceticismo.
- **Esquema *Ponzi* / Pirâmide:** Muitos golpes de investimento operam como esquemas *Ponzi*, onde os retornos dos investidores mais recentes são usados para pagar os investidores anteriores. Esses esquemas inevitavelmente entram em colapso quando não há investidores suficientes para sustentar os pagamentos, deixando a maioria dos investidores com perdas significativas.
- **Vendas Sob Pressão e Táticas de Persuasão:** Os golpistas de investimento muitas vezes usam táticas de vendas agressivas e persuasivas para convencer as pessoas a investir rapidamente, sem fazer a devida diligência. Eles podem criar um senso de urgência, pressionando os investidores a agir imediatamente antes que a oportunidade seja perdida.
- **Falta de Transparência e Informações Enganosas:** Os golpistas geralmente fornecem informações falsas ou enganosas sobre o investimento, ocultando detalhes importantes sobre como o dinheiro será realmente usado ou investido. Eles podem apresentar documentos falsificados, relatórios financeiros fabricados ou até mesmo criar empresas fictícias para dar a aparência de legitimidade.

5.2.3 GOLPES DE FALSIFICAÇÃO DE IDENTIDADE

Esse tipo de fraude envolve o uso indevido das informações pessoais de uma pessoa para obter benefícios financeiros, acesso a serviços ou realizar atividades ilegais em seu nome.

Existem várias maneiras pelas quais os golpistas podem obter informações pessoais de suas vítimas. Isso pode incluir a obtenção de documentos roubados, como carteiras de identidade, passaportes ou cartões de crédito, através de invasões de sistemas informatizados, *phishing* (e-mails falsos que solicitam informações pessoais), roubo de correspondência ou até mesmo através de redes sociais, onde muitas pessoas compartilham informações pessoais sem pensar nas consequências.

Uma vez que os golpistas tenham acesso às informações pessoais de uma vítima, eles podem usá-las de várias maneiras, tais como:

- **Fraude financeira:** Os golpistas podem usar as informações para abrir contas bancárias, obter cartões de crédito, empréstimos ou fazer compras online em nome da vítima.
- **Roubo de identidade:** Os golpistas podem usar as informações pessoais da vítima para se passarem por ela em transações online, contratos ou mesmo cometer crimes, deixando a vítima com sérios problemas legais.
- **Fraude de seguro:** As informações pessoais da vítima podem ser usadas para apresentar reclamações falsas de seguro, resultando em perdas financeiras para as seguradoras e, potencialmente, em aumentos de prêmios para todos os segurados.
- **Fraude de benefícios sociais:** Os golpistas podem se inscrever para benefícios governamentais, como seguro-desemprego ou assistência social, usando as informações pessoais da vítima.
- **Acesso ilegal a serviços online:** Os golpistas podem usar as informações pessoais da vítima para acessar contas online, como e-mails, redes sociais ou serviços de *streaming*, comprometendo a privacidade e a segurança da vítima.

Para proteger-se contra golpes de falsificação de identidade, é importante estar ciente das ameaças e tomar medidas para proteger suas informações pessoais. Isso

inclui não compartilhar informações sensíveis online ou por telefone, verificar regularmente seus extratos bancários e de cartão de crédito em busca de atividades suspeitas, usar senhas fortes e únicas para contas online e estar atento a sinais de alerta de possíveis fraudes, como contas ou cobranças desconhecidas.

Além disso, as empresas e instituições também têm um papel importante a desempenhar na prevenção da falsificação de identidade, implementando medidas de segurança robustas, como a autenticação em duas etapas e a criptografia de dados, e educando seus clientes sobre os riscos e as medidas preventivas disponíveis.

5.2.4 RAMSONWARE

O *ransomware* é uma forma de *malware* que criptografa os arquivos de um sistema de computador e exige um resgate para descriptografá-los. Ele é distribuído principalmente por meio de e-mails de *phishing*, downloads de software malicioso ou exploração de vulnerabilidades em sistemas de computador. Uma vez que o *malware* infecta um sistema, ele começa a criptografar os arquivos do usuário, tornando-os inacessíveis. Em seguida, exibe uma mensagem exigindo o pagamento de um resgate em troca da chave de descriptografia necessária para restaurar os arquivos.

Os ataques de *ransomware* podem ter sérias consequências para as vítimas. Empresas podem perder acesso a dados cruciais, interrompendo operações comerciais e causando perdas financeiras significativas. Para usuários individuais, o impacto também pode ser devastador, especialmente se arquivos pessoais importantes, como fotos, vídeos ou documentos, forem perdidos.

Existem diferentes tipos de *ransomware*, desde variantes relativamente simples até sofisticadas cepas desenvolvidas por grupos de hackers profissionais. Alguns *ransomwares* são projetados para atacar alvos específicos, como organizações governamentais ou empresas de saúde, enquanto outros têm como alvo uma ampla gama de vítimas.

Para se proteger contra ataques de *ransomware*, é importante adotar boas práticas de segurança cibernética, tais como:

- Manter o software atualizado
- Usar software de segurança

- Fazer backups regulares
- Ter cuidado com e-mails e downloads
- Utilizar ferramentas de filtragem de spam
- Educar os usuários

Embora não haja garantia absoluta contra ataques de *ransomware*, seguir essas práticas pode ajudar a reduzir significativamente o risco e minimizar o impacto caso você se torne uma vítima. Além disso, é fundamental ter um plano de resposta a incidentes em vigor para lidar com qualquer ataque de forma eficaz e mitigar seus efeitos.

5.2.5 GOLPES DE COMPRAS ONLINE

Esses golpes podem assumir várias formas e geralmente visam enganar os consumidores, roubar informações financeiras ou vender produtos falsificados. Os golpistas enviam e-mails falsos, mensagens de texto ou anúncios online que parecem ser de empresas legítimas, solicitando informações pessoais ou financeiras. Os consumidores podem ser levados a fornecer dados como números de cartão de crédito, senhas ou informações de conta bancária, que são então usadas para cometer fraudes.

Os golpistas criam sites de comércio eletrônicos falsos que se parecem com lojas online legítimas, oferecendo produtos a preços muito baixos. Os consumidores podem fazer pedidos e fornecer informações de pagamento, apenas para nunca receber os produtos ou receber produtos falsificados ou de baixa qualidade.

Durante o processo de *checkout* em sites legítimos, os golpistas podem interceptar informações de pagamento, como números de cartão de crédito, usando técnicas como ataques de interceptação de dados ou *malware*.

Em plataformas de comércio eletrônico, como Amazon ou eBay, os golpistas podem criar contas falsas de vendedores para listar produtos inexistentes ou falsificados. Os consumidores podem pagar pelos produtos, mas nunca os receberão ou receberão produtos de baixa qualidade.

Anúncios falsos ou promessas enganosas de descontos e ofertas especiais são feitos para atrair consumidores desavisados a clicar em links maliciosos ou a

compartilhar informações pessoais. Para proteger-se contra golpes em compras online, é importante adotar práticas de segurança cibernéticas sólidas, tais como:

- **Verificar a autenticidade do site:** Certifique-se de que está comprando em sites de comércio eletrônicos confiáveis e seguros. Procure por sinais de segurança, como URLs começando com **"https://"** e selos de segurança.
- **Usar métodos de pagamento seguros:** Prefira utilizar métodos de pagamento seguros, como cartões de crédito com proteção contra fraudes, em vez de transferências bancárias ou métodos de pagamento não seguros.
- **Pesquisar e verificar os vendedores:** Antes de comprar de um vendedor desconhecido em um mercado online, pesquise sua reputação e leia comentários de outros compradores.
- **Desconfiar de ofertas muito boas para serem verdadeiras:** Se uma oferta parecer suspeita ou muito boa para ser verdadeira, é provável que seja uma tentativa de golpe.

5.3 ENGENHARIA SOCIAL

A engenharia social envolve a exploração da confiança, da curiosidade, do medo e de outros aspectos psicológicos das pessoas para induzi-las a realizar ações que beneficiem o golpista.

- **Exploração da Confiança:** Muitos golpes de engenharia social se baseiam na criação de uma aparência de legitimidade e confiança. Os golpistas podem se fazer passar por autoridades governamentais, empresas conhecidas, amigos ou familiares para convencer as vítimas a compartilhar informações pessoais ou realizar transações financeiras.
- **Manipulação Emocional:** Os golpistas frequentemente apelam para as emoções das vítimas, como medo, ganância, curiosidade ou compaixão. Eles criam histórias convincentes e urgentes para instigar uma resposta emocional rápida, levando as pessoas a agir sem pensar.
- **Uso de Táticas de Persuasão:** A persuasão desempenha um papel fundamental na engenharia social. Os golpistas podem usar técnicas como

autoridade (fazendo-se passar por uma figura de autoridade), escassez (criando a ilusão de que há uma oferta limitada) e reciprocidade (oferecendo algo em troca) para influenciar o comportamento das vítimas.

- **Exploração da Curiosidade e Ignorância:** Os golpistas muitas vezes contam com a curiosidade natural das pessoas para engajá-las em golpes. Eles podem enviar e-mails ou mensagens intrigantes, como “você ganhou um prêmio” ou “veja quem está falando mal de você”, para atrair as vítimas a clicar em links maliciosos ou fornecer informações pessoais.
- **Métodos de Ataque Variados:** A engenharia social pode ser usada em uma ampla variedade de golpes na internet, incluindo *phishing*, golpes de suporte técnico, fraudes de romance, golpes de herança, entre outros. Os golpistas estão sempre inovando e adaptando suas técnicas para enganar as pessoas de novas maneiras.

Em resumo, a engenharia social continua sendo uma ferramenta poderosa nas mãos dos golpistas na internet. Ao compreender como os golpes de engenharia social funcionam e adotar práticas de segurança cibernéticas adequadas, as pessoas podem reduzir significativamente o risco de se tornarem vítimas desses ataques.

5.4 FERRAMENTAS DIGITAIS UTILIZADAS

No mundo tecnológico, fora toda a engenharia social por trás de golpes, existem também softwares que são criados com o objetivo de acessar máquinas e roubar dados do usuário. Também conhecidos como *spyware*, são uma categoria de *malware* projetada para coletar informações pessoais e confidenciais das vítimas sem o seu conhecimento ou consentimento. Esses programas maliciosos podem ser bastante variados em sua funcionalidade e métodos de operação.

- ***Keyloggers*:** Esses programas registram todas as teclas digitadas pelo usuário, permitindo que os hackers capturem informações como senhas, números de cartão de crédito e mensagens privadas. Um exemplo conhecido de *keylogger* é o Zeus Trojan, que foi usado para roubar informações financeiras de milhões de usuários ao longo dos anos.

- **Trojans de Informações:** Trojans de informações são programas maliciosos que coletam uma variedade de dados pessoais da vítima, incluindo informações de login, detalhes de contas bancárias, histórico de navegação e muito mais. Um exemplo notável é o trojan bancário Emotet, que foi usado para roubar dados financeiros e credenciais de login de instituições financeiras em todo o mundo.
- ***Spyware* de Celular:** Softwares de espionagem para dispositivos móveis são projetados para monitorar e coletar informações de smartphones e tablets. Eles podem capturar mensagens de texto, registros de chamadas, localizações GPS, fotos e muito mais. Exemplos incluem o *FlexiSPY* e o *mSpy*, que foram comercializados como ferramentas de monitoramento parental, mas também foram usados para espionagem não autorizada.
- ***Adware* e *Trackers* de Navegador:** Embora nem todos os *adware* sejam maliciosos, alguns podem coletar informações sobre os hábitos de navegação do usuário e transmiti-las para terceiros sem o consentimento do usuário. Esses programas geralmente são embutidos em software aparentemente legítimo e podem ser difíceis de detectar. Além disso, os *trackers* de navegador podem ser usados por empresas de publicidade para coletar dados de navegação e criar perfis de usuário para fins de direcionamento de anúncios.
- ***RATs (Remote Access Trojans):*** *RATs* são programas que concedem aos hackers acesso remoto completo aos computadores das vítimas, permitindo que eles visualizem a tela, capturem teclas digitadas, acessem arquivos e até controlem o sistema remotamente. Exemplos incluem o *BlackShades* e o *Poison Ivy*, que foram usados para espionagem, roubo de dados e ataques de extorsão.

5.5 TÁTICAS DE PREVENÇÃO

A prevenção e conscientização são elementos essenciais na luta contra os golpes sociais, uma vez que muitos desses ataques exploram a falta de conhecimento e vigilância das vítimas. Aqui estão algumas estratégias eficazes de prevenção e conscientização para combater golpes sociais:

- **Educação e Treinamento:** A educação é a pedra angular da prevenção. As organizações e os indivíduos devem ser treinados regularmente sobre os diferentes tipos de golpes sociais, como *phishing*, engenharia social em redes sociais, fraudes de suporte técnico, entre outros. Eles precisam estar cientes dos sinais de alerta e saber como identificar e relatar atividades suspeitas.
- **Conscientização sobre Técnicas de Manipulação:** É importante que as pessoas compreendam as técnicas de manipulação psicológica utilizadas pelos golpistas, como o apelo à autoridade, escassez, urgência e reciprocidade. Conhecendo essas táticas, as pessoas podem estar mais alertas e menos propensas a serem enganadas.
- **Ênfase na Segurança Cibernética:** A conscientização sobre segurança cibernética deve ser integrada em todos os aspectos da vida digital. Isso inclui a importância de criar senhas fortes e únicas, não compartilhar informações pessoais ou financeiras sem verificar a autenticidade da solicitação, manter o software atualizado e utilizar soluções de segurança, como *firewalls* e programas antivírus.
- **Simulações de Phishing e Testes de Conscientização:** As organizações podem realizar simulações de *phishing* para testar a vigilância de seus funcionários e aumentar a conscientização sobre os riscos de *phishing*. Essas simulações ajudam a identificar áreas de fraqueza e fornecem oportunidades de treinamento adicional.
- **Criação de uma Cultura de Segurança:** É fundamental promover uma cultura de segurança em que todos se sintam responsáveis pela proteção de dados e informações pessoais. Isso requer o envolvimento de todos os níveis da organização, desde a liderança até os funcionários de linha de frente.
- **Atualização Contínua:** Os golpistas estão constantemente desenvolvendo novas táticas e técnicas, por isso é crucial que os programas de

conscientização e treinamento sejam atualizados regularmente para refletir as últimas ameaças e tendências.

Em resumo, a prevenção e conscientização são fundamentais para combater os golpes sociais. Ao educar as pessoas sobre os riscos, fornecer treinamento adequado e promover uma cultura de segurança cibernética, é possível reduzir significativamente o impacto desses ataques e proteger tanto os indivíduos quanto as organizações contra ameaças on-line.

6. A PROPOSTA

O estudo propõe analisar dois dados, o primeiro será a coleta de informações para identificar qual foi o tipo de abordagem mais eficaz para induzir alguém a um golpe. Para isso será registrado a origem de acesso (e-mail, mensagem, WhatsApp etc.) e qual a mensagem enviada, sendo alguns assuntos:

- Informe de compra indevida
- Anúncio de prêmios
- Oferta de crédito
- Alerta de invasão de contas

O segundo fator será quais os assuntos o usuário teve mais interesse ao acessar essa plataforma. Nessa plataforma estará uma página com vídeos, links, materiais e telefones úteis que ensinarão ao usuário como identificar e lidar com tentativas de golpes baseadas no tópico 5.6 táticas de prevenção.

Um esboço simples de uma estrutura de página é a seguinte:

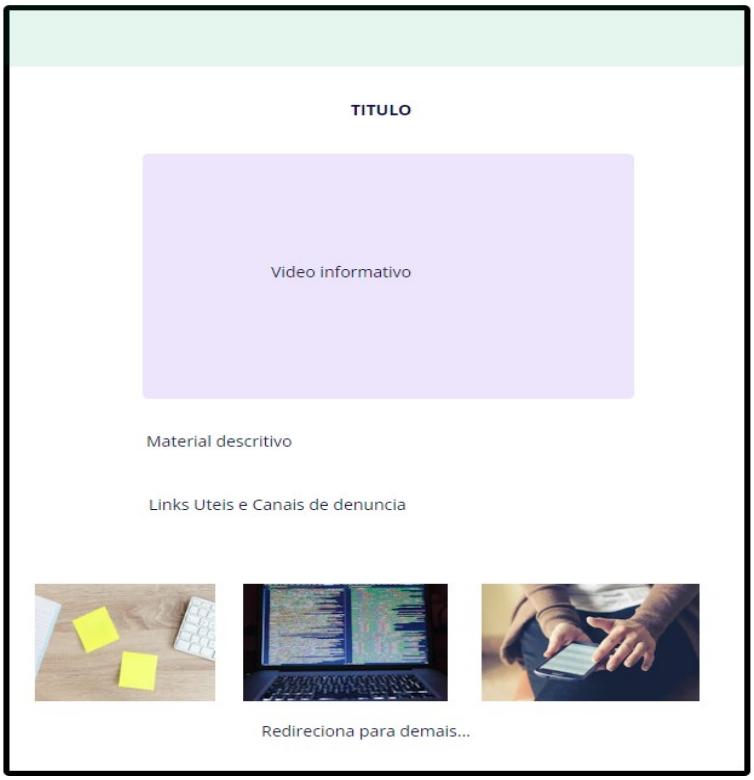

Figura 4 - Esboço da página principal

Para o *frontend* será utilizado o Angular e suas ferramentas para facilitar a criação do design, já o *backend* será em uma *API Rest* em *java* para receber as requisições do *front*.

A expectativa é que ao final poderemos ter números que refletem o comportamento dos usuários ao se deparar com anúncios e mensagens falsas e a partir disso poder direcionar a comunidade em como se prevenir para não serem lesados por golpistas

6.1 TECNOLOGIAS UTILIZADAS

6.1.1 CONCEITO DE API

Uma *API*, ou *Application Programming Interface* (Interface de Programação de Aplicações), é um conjunto de regras, protocolos e ferramentas que permite a comunicação e interação entre diferentes softwares. Ela define como os componentes de software devem interagir uns com os outros, oferecendo uma maneira padronizada e consistente de acesso às funcionalidades ou dados de um sistema para outro. As *APIs* são amplamente utilizadas no desenvolvimento de software por uma série de motivos:

- **Reutilização de código:** Uma *API* permite que desenvolvedores reutilizem funcionalidades existentes em diferentes contextos, sem precisar entender todos os detalhes de como essas funcionalidades são implementadas.
- **Abstração de complexidade:** Uma *API* bem projetada oculta a complexidade interna de um sistema, fornecendo uma interface simples e fácil de entender para os desenvolvedores que desejam interagir com ele.
- **Interoperabilidade:** *APIs* permitem que diferentes sistemas e plataformas interajam entre si, facilitando a integração de sistemas heterogêneos.
- **Facilidade de manutenção:** Ao usar uma *API* para acessar recursos de um sistema, os desenvolvedores podem garantir que suas aplicações continuem funcionando corretamente mesmo que haja mudanças internas no sistema subjacente.
- **Segurança:** As *APIs* podem ser projetadas para fornecer acesso controlado e seguro aos recursos de um sistema, permitindo que os desenvolvedores

imponham restrições de acesso e autentiquem os usuários que desejam interagir com o sistema.

As *APIs* podem assumir diferentes formas, incluindo *APIs* de biblioteca, *APIs* de serviço web, *APIs RESTful*, entre outras. Elas desempenham um papel fundamental no desenvolvimento de software moderno, possibilitando a criação de sistemas complexos e interconectados.

6.1.2 JAVA E SPRING BOOT

Java é uma linguagem de programação de alto nível, orientada a objetos e multiplataforma, criada pela Sun *Microsystems* (adquirida posteriormente pela Oracle Corporation). Ela foi desenvolvida por James Gosling e sua equipe na década de 1990, com o objetivo de ser uma linguagem simples, robusta, portável e segura para o desenvolvimento de software.

Uma das características mais distintivas do *Java* é a sua capacidade de ser executado em diferentes plataformas, graças à sua máquina virtual, conhecida como *JVM (Java Virtual Machine)*. Isso significa que o código *Java* pode ser escrito uma vez e executado em qualquer dispositivo ou sistema operacional que possua uma *JVM* compatível, sem a necessidade de reescrever o código para cada plataforma específica. Principais atributos do *Java*:

- **Orientação a objetos:** *Java* é uma linguagem orientada a objetos, o que significa que todo o código é organizado em classes e objetos, promovendo conceitos como encapsulamento, herança e polimorfismo.
- **Portabilidade:** Graças à *JVM*, os programas *Java* são portáveis e podem ser executados em diferentes plataformas, como *Windows, macOS, Linux* e dispositivos móveis.
- **Sintaxe simples e familiar:** A sintaxe do *Java* é semelhante à de outras linguagens de programação populares, como *C++* e *C#*, facilitando a transição para os desenvolvedores que já estão familiarizados com essas linguagens.
- **Segurança:** *Java* foi projetado com uma série de recursos de segurança, incluindo um sistema de controle de acesso baseado em políticas, que protege contra ameaças como vírus e *malware*.

- **Grande ecossistema e comunidade:** *Java* possui uma vasta biblioteca padrão (API) e uma comunidade ativa de desenvolvedores, o que torna mais fácil encontrar recursos e suporte para o desenvolvimento de software.
- **Ampla utilização:** *Java* é uma das linguagens de programação mais populares e amplamente utilizadas em todo o mundo, sendo empregada em uma variedade de aplicações, desde aplicações web e móveis até sistemas corporativos e embebidos.

Para melhorar e facilitar o desenvolvimento será usado o *framework Spring Boot*. O *Spring Boot* é um *framework* de desenvolvimento de aplicativos *Java* que simplifica significativamente o processo de criação e implantação de aplicativos *Java*. Ele é construído sobre o projeto *Spring*, um dos *frameworks* mais populares e amplamente utilizados no desenvolvimento de aplicativos *Java* empresariais.

A principal filosofia por trás do *Spring Boot* é tornar o desenvolvimento de aplicativos *Java* mais rápido, fácil e eficiente, eliminando a necessidade de configuração manual e reduzindo a quantidade de código *boilerplate* que os desenvolvedores precisam escrever.

Aqui estão alguns dos principais recursos e vantagens do *Spring Boot*:

- **Convenção sobre configuração:** O *Spring Boot* segue o princípio de "convenção sobre configuração", o que significa que ele fornece configurações padrão sensatas para a maioria dos casos de uso. Isso reduz a necessidade de configuração manual e permite que os desenvolvedores iniciem rapidamente sem ter que lidar com detalhes de configuração.
- **Incorporação de servidor de aplicativos:** O *Spring Boot* permite que os aplicativos sejam empacotados como *JARs* executáveis autônomos que incluem um servidor de aplicativos incorporado (como o *Tomcat*, *Jetty* ou *Undertow*). Isso elimina a necessidade de configurar e implantar um servidor de aplicativos separado, simplificando o processo de implantação.
- **Integração perfeita com o ecossistema *Spring*:** O *Spring Boot* é construído sobre o ecossistema *Spring* existente, o que significa que ele se integra perfeitamente com outros projetos *Spring*, como *Spring MVC*, *Spring Data*, *Spring Security* e muito mais. Isso oferece aos desenvolvedores acesso a uma

ampla gama de recursos e funcionalidades para desenvolver aplicativos *Java* de alta qualidade.

- **Configuração externa:** O *Spring Boot* permite que a configuração do aplicativo seja externalizada para arquivos de propriedades, *YAML*, variáveis de ambiente ou qualquer outro mecanismo de configuração suportado. Isso facilita a personalização e a configuração do aplicativo para diferentes ambientes, como desenvolvimento, teste e produção.
- **Facilidade de teste:** O *Spring Boot* facilita a escrita de testes para aplicativos *Java*, fornecendo suporte para testes de unidade, testes de integração e testes de ponta a ponta. Ele também fornece ferramentas integradas para execução de testes e geração de relatórios de cobertura de código.
- **Monitoramento e gerenciamento:** O *Spring Boot* inclui recursos integrados para monitoramento e gerenciamento de aplicativos, como *endpoints* de saúde, métricas, informações de ambiente e muito mais. Isso facilita a monitoração e o diagnóstico de problemas em tempo real.

No geral, o *Spring Boot* é uma escolha popular para o desenvolvimento de aplicativos *Java* devido à sua simplicidade, produtividade e integração perfeita com o ecossistema *Spring*. Ele ajuda os desenvolvedores a criar aplicativos robustos, escaláveis e de fácil manutenção com menos esforço e tempo gasto em configuração e infraestrutura.

6.1.3 POSTGRES

O *PostgreSQL*, também conhecido como *Postgres*, é um sistema de gerenciamento de banco de dados relacional de código aberto e de alta performance. Ele foi desenvolvido originalmente na Universidade da Califórnia, em Berkeley, nos Estados Unidos, e é mantido e continuamente aprimorado por uma comunidade global de desenvolvedores.

O *PostgreSQL* é amplamente elogiado por sua robustez, confiabilidade e conformidade com os padrões *SQL*. Ele oferece uma ampla gama de recursos

avançados que o tornam uma escolha popular para uma variedade de aplicativos, desde pequenos projetos de desenvolvimento até grandes sistemas empresariais.

Algumas das principais características e capacidades do *PostgreSQL*:

- **Modelo de dados relacional:** O *PostgreSQL* é um banco de dados relacional, o que significa que organiza os dados em tabelas com linhas e colunas, seguindo os princípios do modelo relacional.
- **Suporte a *SQL*:** O *PostgreSQL* oferece suporte total ao *SQL* padrão, além de várias extensões e funcionalidades avançadas, como subconsultas, junções, agregações e transações.
- **Integridade de dados:** Ele fornece mecanismos robustos para garantir a integridade e consistência dos dados, incluindo restrições de chave estrangeira, gatilhos e verificações de integridade.
- **Extensibilidade:** O *PostgreSQL* é altamente extensível, permitindo que os usuários adicionem novos tipos de dados, funções, operadores e até mesmo linguagens de programação personalizadas.
- **Replicação e alta disponibilidade:** Ele suporta várias opções de replicação, como replicação síncrona e assíncrona, bem como *failover* automático para garantir alta disponibilidade e tolerância a falhas.
- **Desempenho:** O *PostgreSQL* é conhecido por seu desempenho excepcional, especialmente em cargas de trabalho complexas e de alto volume. Ele oferece otimizações avançadas de consulta, índices, particionamento de tabelas e paralelismo de consulta.
- **Segurança:** O *PostgreSQL* possui recursos avançados de segurança, incluindo autenticação baseada em senha ou certificado, criptografia de dados em repouso e em trânsito, controle de acesso granular e auditoria de atividades.
- **Suporte a geoespacial:** Ele inclui suporte nativo para dados geoespaciais, permitindo armazenar, consultar e analisar dados relacionados a localização geográfica.

6.1.4 ANGULAR

Angular é uma plataforma e estrutura de desenvolvimento de código aberto mantida pelo Google e uma comunidade de desenvolvedores. É amplamente utilizada para criar aplicações web de página única (*SPA - Single Page Applications*) e aplicações web dinâmicas. Aqui estão alguns pontos-chave sobre *Angular*:

- **Arquitetura *MVC*:** Angular segue o padrão de arquitetura *MVC (Model-View-Controller)*, embora com suas próprias abordagens específicas. O modelo representa os dados, a visualização é a interface do usuário e o controlador é responsável pela lógica de negócios.
- ***TypeScript***: *Angular* é desenvolvido com *TypeScript*, uma linguagem de programação *superset* do *JavaScript* que adiciona recursos como tipagem estática, interfaces e outras funcionalidades de programação orientada a objetos. Isso aumenta a robustez e a manutenibilidade do código.
- **Componentes:** *Angular* é baseado em componentes reutilizáveis. Os componentes são blocos de construção fundamentais das aplicações *Angular*, cada um encapsulando sua própria lógica e apresentação. Eles promovem a modularidade e facilitam a manutenção do código.
- ***Data Binding:*** Angular oferece vinculação de dados bidirecional, o que significa que as alterações nos modelos de dados são refletidas automaticamente na interface do usuário e vice-versa. Isso simplifica a manipulação de dados e melhora a responsividade das aplicações.
- **Injeção de Dependência:** *Angular* possui um sistema de injeção de dependência embutido que facilita a criação, teste e manutenção de aplicações. Ele permite que os componentes recebam suas dependências de forma transparente, promovendo a coesão e a reutilização do código.
- **Roteamento:** *Angular* fornece um módulo de roteamento que permite a navegação entre diferentes partes da aplicação. Ele suporta roteamento baseado em URL, permitindo que os usuários naveguem entre diferentes páginas sem recarregar a página inteira.
- **Ferramentas de Desenvolvimento:** Angular é suportado por uma ampla gama de ferramentas e utilitários de desenvolvimento, incluindo o *Angular CLI*

(Command Line Interface) para geração de projetos, criação de componentes e muito mais. Também é integrado com *IDEs* populares como *Visual Studio Code.*

6.1.5 HEROKU

Para disponibilizar a aplicação na rede, foi escolhido o *Heroku* que é uma plataforma de nuvem que permite aos desenvolvedores construírem, executar e escalar aplicações web de forma rápida e fácil. Os motivos pela escolha dessa plataforma foram:

O *Heroku* simplifica o processo de implantação e hospedagem de aplicações web. Com apenas alguns comandos na linha de comando ou cliques no painel de controle, os desenvolvedores podem implantar suas aplicações em questão de minutos. O serviço também oferece suporte a várias linguagens de programação populares, incluindo *Node.js, Ruby, Python, Java, PHP, Go* e mais recentemente, suporte experimental a *Rust* e *Elixir*. Isso permite que os desenvolvedores usem suas linguagens preferidas sem se preocupar com a infraestrutura subjacente.

A plataforma facilita a escalabilidade das aplicações. Os aplicativos podem ser dimensionados verticalmente (adicionando mais recursos, como CPU e memória) ou horizontalmente (adicionando mais instâncias de aplicativos) com apenas alguns cliques ou comandos na linha de comando.

- **Integração com Ferramentas Populares:** O *Heroku* se integra perfeitamente com várias ferramentas populares de desenvolvimento, como *GitHub, GitLab, Docker, Travis CI* e mais. Isso facilita a integração contínua, a entrega contínua (CI/CD) e outras práticas de desenvolvimento ágil.
- **Ecossistema de *Add-ons*:** O *Heroku* possui um ecossistema de *add-ons* que oferece uma ampla gama de serviços complementares, como bancos de dados, cache, monitoramento, análise, segurança e muito mais. Os desenvolvedores podem adicionar e configurar esses serviços com apenas alguns cliques ou comandos.
- **Segurança e Conformidade:** O *Heroku* leva a segurança dos dados dos clientes a sério e oferece uma série de recursos e práticas recomendadas para

garantir a segurança e a conformidade com regulamentações como GDPR, HIPAA e ISO 27001.

6.1.6 QR CODE

Os códigos *QR*, ou *Quick Response codes*, têm sido uma ferramenta extremamente versátil e útil em diversas áreas, desde marketing e publicidade até logística e segurança. Sua popularidade cresceu exponencialmente, especialmente com a proliferação de smartphones e a necessidade de acesso rápido a informações.

Uma das vantagens mais marcantes do *QR code* é a capacidade de armazenar uma grande quantidade de dados em uma pequena área. Isso os torna ideais para transmitir informações de forma eficiente e conveniente, especialmente em situações em que o espaço é limitado, como em anúncios impressos, embalagens de produtos ou cartões de visita.

As áreas mais comuns em que podemos encontrar *QR code* são:

- **Logística e Rastreamento:** Empresas podem usar códigos *QR* para rastrear o movimento de produtos ao longo da cadeia de suprimentos, facilitando a logística e o controle de estoque.
- **Educação:** Educadores podem incorporar códigos *QR* em materiais didáticos para fornecer aos alunos acesso rápido a recursos online, como vídeos, artigos ou exercícios adicionais.
- **Turismo e Informações Locais:** Pontos turísticos, museus e cidades podem usar códigos *QR* em placas informativas para fornecer aos visitantes acesso a informações detalhadas sobre locais específicos.
- **Segurança:** Os códigos *QR* podem ser usados para autenticação e verificação de identidade em sistemas de segurança, como bilhetes de eventos ou passes de transporte.

No entanto, apesar de sua utilidade, os códigos *QR* também apresentam desafios e preocupações. Por exemplo, eles podem ser explorados por pessoas mal-intencionadas para direcionar usuários a sites maliciosos ou *phishing*. Portanto, é importante que os usuários estejam cientes dos riscos ao escanear códigos *QR* de

fontes não confiáveis e que as empresas adotem medidas de segurança adequadas ao implementar códigos *QR* em seus materiais.

6.1.7 DOCKER

Docker é uma plataforma de código aberto que facilita a criação, implantação e execução de aplicativos em contêineres. Mas o que são contêineres? Eles são ambientes isolados que encapsulam um aplicativo e todas as suas dependências, como bibliotecas e configurações, permitindo que eles sejam executados de maneira consistente em qualquer ambiente. Uma das principais vantagens do *Docker* é a portabilidade. Como os contêineres contêm tudo o que um aplicativo precisa para ser executado, eles podem ser movidos facilmente entre diferentes ambientes, desde o desenvolvimento até a produção, garantindo consistência e reduzindo problemas de "funciona na minha máquina".

O *Docker* simplifica o processo de implantação de aplicativos. Com *Docker*, você pode definir a infraestrutura necessária para executar seu aplicativo em um arquivo chamado *Dockerfile*, que descreve todas as etapas necessárias para construir uma imagem *Docker*. Essa imagem pode então ser compartilhada e implantada em qualquer ambiente compatível com *Docker*.

Outra vantagem do *Docker* é a eficiência de recursos. Como os contêineres compartilham o *kernel* do sistema operacional subjacente, eles são muito mais leves em comparação com máquinas virtuais tradicionais, o que significa que você pode executar mais contêineres em uma única máquina, economizando recursos e reduzindo custos.

Além disso, o *Docker* facilita a escalabilidade. Com ferramentas como *Docker Swarm* e *Kubernetes*, você pode automatizar o dimensionamento de seus aplicativos com base na demanda, garantindo que eles permaneçam disponíveis e responsivos, independentemente do número de usuários.

7. CRONOGRAMA

Um cronograma é uma representação visual ou escrita de uma sequência de eventos, atividades ou tarefas planejadas ao longo do tempo. É uma ferramenta essencial para o gerenciamento de projetos, planejamento de eventos, organização de tarefas pessoais e muitas outras atividades que envolvem a alocação de recursos e a coordenação de atividades ao longo de um período específico. Os cronogramas geralmente incluem uma lista de atividades ou marcos importantes que precisam ser realizados, com suas datas de início e término previstas.

Atividades	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov
Pesquisa do tema									
Definição do tema									
Pesquisa bibliográfica									
Coleta de Dados									
Apresentação e discussão dos dados									
Elaboração do projeto									
Entrega do projeto									

Figura 4: Cronograma

	Feito
	Em Andamento
	Planejado
	Atrasado

Figura 5: Legenda do cronograma

8. CONCLUSÃO

Com todos os dados apresentados foi possível obter uma dimensão do problema enfrentado que se deu pela expansão da internet e os meios de comunicação. Da última década até hoje a maior parte da população brasileira conseguiu acesso à internet e outros recursos de comunicação, esses que por sua vez facilitam a vida no dia a dia também abrem portas para outros perigos que muitas vezes as pessoas não estão preparadas para enfrentá-los. É muito comum ouvir relatos de amigos e familiares que caíram em golpes na internet e a engenharia social por trás está sempre criando métodos de tornar a abordagem mais convincente para enganar as vítimas.

Cabe em uma força conjunta de órgãos governamentais, empresas privadas e a população espalhar informações e conscientizar a sociedade para tornar-se mais críticas ao analisar mensagens e anúncios, procurando encontrar padrões que indiquem uma má intenção de quem envia o golpe.

A proposta de criar uma plataforma de conscientização cria a expectativa de fazer esse serviço a comunidade e conseguir coletar informações de como as pessoas se comportam ao serem abordadas por essas tentativas de golpes, assim criar uma base de estudo para atacar o problema com mais eficiência.

9. REFERÊNCIAS

PATRICIA.SANKARI. **Docente publica artigo sobre golpe virtual no Estadão – Portal de Notícias da Cruzeiro do Sul Educacional**. Disponível em: <https://noticias.cruzeirodosuleducacional.edu.br/docente-publica-artigo-sobre-golpe-virtual-no-estadao/>. Acesso em: 17 mar. 2024.

KAPERSKY. **Brasil é o país com mais ataques a dispositivos móveis na América Latina**. Disponível em: <https://www.kaspersky.com.br/blog/brasil-recebe-mais-ataques-america-latina/21782/>. Acesso em: 15 abr. 2024.

GUSSON, CASSIO. **Com 103,1 bilhões de tentativas de ataque virtual, Brasil é o segundo país que mais sofre com crimes cibernéticos na América Latina**. Disponível em: <https://br.cointelegraph.com/news/brazil-is-the-second-country-that-suffers-the-most-cyber-attacks-in-latin-america>. Acesso em: 20 abr. 2024.

PIERRE, JEAN. **Não caia mais em golpes na internet: conheça os 6 mais comuns e saiba como se proteger!** Disponível em: <https://www.jusbrasil.com.br/artigos/nao-caia-mais-em-golpes-na-internet-conheca-os-6-mais-comuns-e-saiba-como-se-proteger/1830693006>. Acesso em: 25 abr. 2024.

JAVA. **What is Java technology and why do I need it?** Disponível em: <https://www.java.com/en/download/help/whatis_java.html>. Acesso em: 25 abr. 2024.

JAVA. **Java: o que é, linguagem e Guia para iniciar na tecnologia**. Disponível em: <https://www.alura.com.br/artigos/java>. Acesso em: 20 mar. 2024.

ALURA. **Angular: o que é, para que serve e um Guia do framework**. Disponível em: <https://www.alura.com.br/artigos/angular-js?utm_term=&utm_campaign=%Search%5D+%5BPerformance%5D+-+Dynamic+Search+Ads+-+Artigos+e+Conte>. Acesso em: 2 mai. 2024.

REDHAT. **Docker | O que é Docker e como ele funciona?** Disponível em: <https://www.redhat.com/pt-br/topics/containers/what-is-docker>. Acesso em: 12 mar. 2024.

KAPERSKY**. Um guia sobre códigos QR e como fazer sua leitura**. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-a-qr-code-how-to-scan#:~:text=Quais%20s>. Acesso em: 20 mar. 2024.

SPRING. **Spring Projects.** Disponível em: <https://spring.io/projects/spring-boot>. Acesso em: 25 abr. 2024.

EINVESTIDOR. **Golpes financeiros crescem no mundo. Saiba como não perder dinheiro**. Disponível em: <https://einvestidor.estadao.com.br/colunas/eduardo-mira/como-nao-perder-dinheiro-em-golpes-financeiros/>. Acesso em: 2 abr. 2024.

ECOMMERCE BRASIL. **No Brasil, 80 mil pessoas já foram vítimas de golpes online em 2023**. Disponível em: <https://www.ecommercebrasil.com.br/noticias/no-brasil-80-mil-pessoas-ja-foram-vitimas-de-golpes-online-em-2023>. Acesso em: 4 abr. 2024

ESTADO DE MINAS. **Pesquisa revela: 71% dos brasileiros já foram vítimas de golpes virtuais**. Disponível em: <https://www.em.com.br/app/noticia/tecnologia/2023/07/11/interna_tecnologia,1518903/pesquisa-revela-71-dos-brasileiros-ja-foram-vitimas-de-golpes-virtuais.shtml>. Acesso em: 5 abr. 2024.

SOUZA, B. DE A.; JACOB, R. R. C. **Golpes Digitais – Ed. 2024**. Disponível em: <https://www.jusbrasil.com.br/doutrina/secao/4-principais-motivacoes-por-tras-dos-crimes-parte-i-compreendendo-os-golpes-digitais-golpes-digitais-ed-2024/2485204980>. Acesso em: 10 abr. 2024.

UOL. **Brasileiros sofrem 208 golpes por hora; alta é de 37,9%**. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2023/07/20/puxado-por-golpes-eletronicos-estelionatos-sobem-379-homicidios-caem.htm>. Acesso em 30 abr. 2024

DIGITAL, O.; GOMEZ, V. L. Golpe: **Brasil é o segundo país com mais crimes digitais no mundo**. Disponível em: <https://olhardigital.com.br/2023/10/27/seguranca/golpe-brasil-e-o-segundo-pais-com-mais-crimes-digitais-no-mundo/>. Acesso em: 15 mai. 2024.

GLOBO. **9 de 10 golpes na internet têm motivação financeira, aponta estudo**. Disponível em: <https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2020/06/12/9-em-cada-10-golpes-na-internet-tem-motivacao-financeira-aponta-estudo.ghtml>. Acesso em: 20 mai. 2024.

G1. **Tentativas de golpes por meios digitais cresceram 20% no segundo trimestre deste ano no Brasil**. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/10/11/tentativas-de-golpes-por-meios-digitais-cresceram-20percent-no-segundo-trimestre-deste-ano-no-brasil.ghtml>. Acesso em: 20 mai. 2024

G1. **Estelionatos no Brasil mais que quadruplicam em cinco anos, e golpes virtuais disparam após pandemia, revela Anuário**. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2023/07/20/estelionatos-no-brasil-mais-que-triplicam-em-cinco-anos-e-golpes-virtuais-disparam-apos-pandemia-revela-anuario.ghtml>. Acesso em: 20 mai. 2024

KAPERSKY**. Com retomada econômica e IA, phishing cresce mais de 5 vezes no Brasil**. Disponível em: <https://www.kaspersky.com.br/blog/panorama-de-ciberameacas-2023/21631/#:~:text=Em%202022%2C%20os%20golpes%20de>. Acesso em: Acesso em: 25 mai. 2024.

FOLHA. **Entre 2013 e 2023, número de usuários de internet no Brasil aumentou 78%**. Disponível em: <https://piaui.folha.uol.com.br/entre-2013-e-2023-numero-de-usuarios-de-internet-no-brasil-aumentou-78/#:~:text=Dez%20anos%20atr%C3%A1s%2C%20102%20milh%C3%B5es>. Acesso em: 25 mai. 2024.

KAPERSKY. **Quais são os principais golpes online e como evitá-los?** Disponível em: <https://www.kaspersky.com.br/resource-center/threats/top-scams-how-to-avoid-becoming-a-victim>. Acesso em: 20 mai. 2024.

CHECK POINT. **Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most** Disponível em: <https://www.kaspersky.com.br/resource-center/threats/top-scams-how-to-avoid-becoming-a-victim>. Acesso em: 20 mai. 2024.