COLÉGIO ESTADUAL DE CONCEIÇÃO DO JACUÍPE

ENSINO MÉDIO INTEGRADO AO CURSO TÉCNICO EM INFORMÁTICA

DAVI PACHECO RIOS
BRUNO DOS SANTOS MOREIRA
MARIA EDUARDA DA CONCEIÇÃO

GOLPES VIRTUAIS: ORIENTAÇÃO SOBRE SEGURANÇA DA INFORMAÇÃO

Conceição do Jacuípe - BA
2023

DAVI PACHECO RIOS
BRUNO DOS SANTOS MOREIRA
MARIA EDUARDA DA CONCEIÇÃO

GOLPES VIRTUAIS: ORIENTAÇÃO SOBRE SEGURANÇA DA INFORMAÇÃO

Trabalho de conclusão de curso apresentado ao curso em Técnico de informática, do Colégio Estadual de Conceição do Jacuípe, para obtenção do grau de Técnico de Informática. Orientadora: Prof. Jadiane Santana

Conceição do Jacuípe - BA
2023

SUMÁRIO

SUMÁRIO DAS FIGURAS

1 INTRODUÇÃO

A segurança da informação é uma área cada vez mais importante no mundo digital. Com a crescente utilização de dispositivos conectados à internet, a troca de informações e dados pessoais se tornou uma prática diária para muitas pessoas e empresas.

A segurança da informação trata de garantir a confidencialidade, integridade e disponibilidade das informações, ou seja, proteger os dados de acesso não autorizado, alterações indevidas e indisponibilidades. A segurança da informação é um conjunto de medidas que visa proteger as informações de possíveis ameaças e vulnerabilidades, tais como vírus, *malwares, phishing*, ataques de hackers, entre outros. A importância da segurança da informação está relacionada à proteção das informações sensíveis, como dados pessoais, informações financeiras, senhas e documentos sigilosos. Além disso, uma violação da segurança da informação pode causar danos irreparáveis à imagem da empresa, perda de clientes e prejuízos financeiros. Por isso, é fundamental que as empresas e os indivíduos se conscientizem da importância da segurança da informação e adotem medidas preventivas.

Com o avanço da tecnologia, os golpes virtuais se tornaram cada vez mais comuns e sofisticados, esses golpes são influenciados por criminosos que se aproveitam da ingenuidade e falta de conhecimento das pessoas para obter informações pessoais, financeiras e até mesmo cometer crimes cibernéticos. Diante desses acontecimentos, é de extrema importância saber, quais são os principais golpes virtuais e como evitá-los?

Existem várias formas de golpes virtuais, desde *phishing*, onde o criminoso se passa por uma empresa legítima para obter informações pessoais e financeiras, até mesmo os golpes de *ransomware*, onde o criminoso bloqueia o acesso aos dados do usuário e exige um resgate para liberá-los. Com o aumento do uso da internet, os golpes virtuais tornaram-se uma ameaça constante para a população, que muitas vezes desconhece as melhores práticas para se proteger. Nesse sentido, a pesquisa em questão tem como objetivo geral, trazer informações a fim de mostrar à população a importância da segurança da informação, trazer orientações sobre

como evitar cair em golpes virtuais. E com isso os objetivos específicos desta pesquisa é: apresentar os principais golpes mais comuns na internet; apresentar formas de evitar golpes virtuais; criar como produto um site orientando sobre formas de evitar golpes virtuais, utilizando a plataforma da *Hostinger*. Assim por meio da criação deste site, espera-se que mais pessoas se tornem conscientes dos riscos envolvidos na navegação na internet e adotem medidas para se protegerem contra possíveis ataques e fraudes virtuais.

Esta pesquisa tem uma abordagem quali-quantitativa. É uma abordagem de pesquisa que combina elementos da pesquisa qualitativa e quantitativa. A pesquisa qualitativa busca compreender e analisar detalhadamente as experiências e vivências dos indivíduos, enquanto a pesquisa quantitativa busca medir estatísticas para obter resultados precisos com base em dados numéricos. A abordagem quali-quantitativa visa obter uma compreensão ampla e detalhada do fenômeno em estudo. A pesquisa será de natureza bibliográfica e exploratória, utilizando estudos de livros e artigos científicos para levantar informações, identificar padrões e estabelecer bases conceituais preliminares, com o objetivo de gerar insights e orientar pesquisas futuras mais aprofundadas. Utilizando a abordagem quali-quantitativa e a pesquisa de natureza bibliográfica e exploratória, o trabalho cientifico terá como produto a criação de um site por meio da plataforma da Hostinger, que ofereça um conteúdo abrangente sobre segurança da informação, especialmente direcionado àqueles que possuem pouco conhecimento sobre o assunto. Esse site terá como propósito ampliar a conscientização e o entendimento da sociedade em relação à segurança da informação.

2. REFERENCIAL TEORICO

Nos últimos tempos a internet tem sido alvo de muitos ataques cibernéticos com isso as grandes empresas procuram aumento da segurança da informação para usuários internos e externos com os serviços bancários online ou comércio eletrônico há necessidade de proteger informações críticas cresceu proporcionalmente. O universo de conteúdos digitais está cada vez mais suscetível a ameaças que comprometem a segurança das pessoas e das informações Marciano (2006 p16). Essas ameaças são ainda mais complexas no caso da autenticação na internet, pois envolvem fatores além do controle do serviço de segurança, como o hardware e os sistemas operacionais do usuário (RANGHETTI, MILNITSKY p.48, 2007). Portanto, é fundamental compreender a complexidade do usuário, sistema e informação para implementar medidas adequadas de segurança na internet e garantir a proteção das informações confidenciais. A segurança da informação tem como objetivo garantir a confidencialidade, integridade e disponibilidade dos dados. A confidencialidade refere-se ao acesso restrito apenas a pessoas autorizadas, evitando a divulgação não autorizada. A integridade diz respeito à preservação da precisão e integridade dos dados, evitando alterações não autorizadas. Sendo assim campo crucial no ambiente digital atual, onde a dependência crescente da tecnologia e o fluxo constante de dados alcançaram uma necessidade maior de proteção das informações uma prioridade para indivíduos e empresas. Como apresentado no gráfico da Gráfico 1.

Grafico1-Vulnerabilidades e incidentes de segurança da informação em sites no mundo reportados no período de 1988 a 2003

Fonte: CERT (2004)

Existem várias ameaças que comprometem a segurança da informação. Os *malwares* representam uma das principais ameaças à segurança da informação sendo uma ameaça persistente e em constante evolução, que segundo (NIC. BR, 2012) malwares são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Existem vários tipos de malwares os principais deles são: vírus que conforme (NIC. BR, 2012) é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo copias de si mesmo e se tornando parte de outros programas e arquivos, para (NIC. BR, 2012) o *Worm* que diferente do vírus, *o worm* não se propaga por meio da inclusão de copias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores, segundo (NIC. BR, 2012) O spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros, (NIC.BR, 2012). De acordo com (NIC. BR, 2012) *Backdoor* é um programa que permite ó retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo. Conforme (NIC.BR, 2012) Cavalo de Tróia ou trojan é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário. E o *phishing* que de acordo com (NIC.BR, 2012) *phishing* é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário. Além do malwares, o fator humano também são grandes causadores de riscos, como o descuido ou a má conduta dos usuários, também podem expor as informações a ameaças internas. É fundamental compreender essas ameaças e suas origens para implementar medidas adotadas de proteção.

Existem princípios e medidas essenciais para proteger a informação. A autenticação, por exemplo, garante que apenas usuários autorizados tenham acesso aos dados, através de senhas, autenticação de dois fatores ou outros métodos. As

senhas são uma das principais medidas de proteção utilizadas para garantir a segurança das informações confidenciais. A segurança de uma senha é frequentemente avaliada com base em sua complexidade. Tradicionalmente, acredita-se que uma senha segura deve incluir uma combinação de letras maiúsculas e minúsculas, números e símbolos. No entanto, descobriu-se que o comprimento da senha é mais importante do que a sua complexidade. Portanto, frases secretas são consideradas as melhores opções de senha. É mais fácil para um hacker habilidoso decifrar uma senha curta e complexa do que uma senha longa, mesmo que esta última seja composta apenas por letras minúsculas (FIA, 2022),é importante manter as senhas em sigilo e trocá-las regularmente, conforme necessário, para aumentar a segurança dos dados e minimizar as chances de invasões (RANGHETTI, MILNITSKY,p47.2007).Mas de suma importância esclarecer que quanto maior e complexa a senha levará uma maior perca de tempo por parte do invasor para quebra a senha do usuário como mostrado na tabela abaixo.

Tabela 1 – Nível de segurança das senhas

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years

Fonte: https://www.hivesystems.io/blog/are-your-passwords-in-the-green

A implementação de medidas adicionais de segurança, como a autenticação em dois fatores e o uso de softwares antivírus atualizados, também pode ser útil para a segurança de dados. No entanto, muitos intrusos, também conhecidos como hackers, tentam comprometer o sistema da empresa, e os ataques estão se tornando cada vez mais comuns, atingindo desde grandes empresas até indivíduos comuns (RANGHETTI, MILNITSKY, p47. 2007).

A fim de evitar a infecção por malwares, é fundamental estar atento aos seguintes aspectos: o download de softwares gratuitos sejam eles legítimos ou não; o acesso a web sites infectados; a clicar em falsas mensagens de erro ou janelas de pop-up; e a abrir e-mails suspeitos. Ao adotar uma postura cautelosa e consciente nessas situações, é possível reduzir significativamente o risco de ser afetado por malwares. Além de adotar precauções com as medidas mencionadas anteriormente, é importante contar com um antivírus confiável instalado em seu computador e manter regularmente o sistema operacional atualizado. O antivírus desempenha um papel fundamental ao analisar e verificar possíveis *malwares* em itens de download antes de sua abertura, garantindo assim uma camada adicional de proteção.

Para fortalecer a segurança da informação, é importante adotar boas práticas. Isso inclui manter sistemas e software atualizados, realizar backups regularmente, promover uma cultura de conscientização e treinamento em segurança da informação entre os usuários. Isso pode incluir a realização de palestras, workshops e distribuição de materiais educativos para ensinar boas práticas, como evitar clicar em links suspeitos, não compartilhar senhas, proteger dispositivos móveis e estar atento a tentativas de *phishing*, A implementação de políticas de segurança claras e abrangentes também desempenha um papel fundamental na proteção da informação. Essas políticas devem abordar questões como o uso adequado dos recursos digitais, a criação de senhas fortes, a restrição de acesso a dados e por fim, é essencial monitorar constantemente possíveis ameaças e estar preparado para responder a incidente de segurança. Isso envolve a implementação de sistemas de detecção de intrusões, análise de logs de eventos, monitoramento de tráfego de rede e criação de um plano de resposta a incidentes que estabeleça procedimentos claros para lidar com possíveis violações de segurança. Ao adotar essas boas práticas, as organizações podem fortalecer significativamente sua postura de segurança da informação, acolher os respeitos de respeito, perdas de dados e danos à confiança. A segurança da informação deve ser encarada como um esforço contínuo, envolvendo a colaboração de todos os usuários e a adoção de medidas proativas para enfrentar as ameaças digitais em constante evolução.

3. METODOLOGIA

Essa pesquisa possui caráter exploratório e bibliográfico. A pesquisa bibliográfica é o levantamento ou revisão de obras publicadas sobre a teoria que ira direcionar o trabalho cientifico o que necessita uma dedicação, estudo e analise pelo pesquisador que irá executar o trabalho cientifica e tem como objetivo reunir e analisar texto publicado para apoiar o trabalho (CARLOS GIL, 2002). A pesquisa exploratória segundo Gil (2002) tem como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a conseguir hipóteses. Com isso essa pesquisa usar de fontes bibliográficas para compreensão do tema e utilizá-los na construção de um site com objetivo de tornar conteúdo da segurança da informação mais amplo para sociedade com alvo naqueles que compreendem pouco sobre o assunto.

Este trabalho de pesquisa tem uma abordagem quali-quantitativa. Essa abordagem busca entender um fenômeno de maneira mais completa e aprofundada, por meio da coleta e análise de dados qualitativos e quantitativos. Na pesquisa quali-quantitativa, são utilizadas técnicas tanto da pesquisa qualitativa, que foca na compreensão dos significados, experimentação e experiência dos indivíduos, quanto da pesquisa quantitativa, que utiliza a mensuração e a análise estatística para obter resultados mais precisos e generalizáveis (GERHAQRAT e SILVEIRA. 2009). Dessa forma, a pesquisa quali-quantitativa busca obter uma compreensão mais ampla e integrada do fenômeno estudado, permitindo uma análise mais completa das suas diferentes perspectivas e dimensões. Nesse sentido, a pesquisa proposta realizará uma coleta de dados embasada em artigos científicos conceituados, bem como em sites especializados que abordam os principais golpes virtuais e oferecem medidas preventivas para evitá-los.

É importante ressaltar que o intuito final dessa pesquisa é a criação de um site que sirva como um repositório de informações confiáveis e atualizadas sobre o tema. Esse site terá como propósito principal expor todos os dados coletados, fornecendo um recurso valioso para aqueles que desejam se informar e se proteger contra os diferentes tipos de golpes virtuais existentes. Afinal, a conscientização e a adoção de medidas preventivas são fundamentais para evitar prejuízos financeiros e proteger a privacidade e a segurança digital dos usuários da internet.

3.1 Os principais golpes mais comuns na internet

Malware é a abreviação de "software malicioso" (em inglês, *malicious* software) e se refere a um tipo de programa de computador desenvolvido para infectar o computador de um usuário legítimo e prejudicá-lo de diversas formas. O *malware* pode infectar computadores e dispositivos de várias maneiras, além de assumir diversas formas, entre elas vírus, *worms*, cavalos de troia, *spyware* e outros. É importante que todos os usuários saibam como reconhecer e se proteger do malware em todas as suas formas

Phishing: é uma forma de ataque que visa enganar pessoas para obter informações confidenciais. Os ataques de *phishing* geralmente ocorrem com hacker se passando por entidades confiáveis, como bancos, empresas e serviços online populares, com o intuito de ganhar a confiança da vítima. Esses golpes são geralmente realizados por meio de e-mails, mensagens de texto, mensagens instantâneas ou páginas web falsas que se assemelham aos sites legítimos. Eles costumam conter links maliciosos ou solicitam que a vítima insira suas informações pessoais em formulários falsos. Ao cair numa página de *phishing*, a vítima pode desavisada mente revelar seus dados confidenciais aos hackers, podendo usar seus dados para cometer fraudes, roubo de identidade ou cometendo outros tipos de crimes.

Figura 1-Imagem ilustrativa de *phishing*

Fonte: https://segredosdomundo.r7.com/o-que-e-phishing/

Trojan: também conhecido como cavalo de Tróia, é um tipo de *malware* (software malicioso) que se disfarça como um programa legítimo ou inofensivo para enganar os usuários e infectar seus dispositivos. Assim como o cavalo de Tróia da mitologia grega, que foi usado para infiltrar soldados dentro das muralhas da cidade de Tróia,

o *Trojan* é projetado para se infiltrar nos sistemas dos usuários de forma oculta e maliciosa. Os *Trojans* podem se apresentar como programas aparentemente úteis, como jogos, utilitários, atualizações de software ou até mesmo documentos atraentes. Eles podem ser distribuídos por e-mail, links maliciosos, downloads de fontes não confiáveis ou mesmo por meio de mídias removíveis, como *pendrives*.

Figura 2- Ilustração sobre Trojan

Fonte: https://aratecnia.es/definicion-virus-informatico/

Keylogger: é vírus que quando invadir um computador captar todas as teclas que são usadas que são enviadas para o cyber criminoso. Não só de crime vive o *keylogger* eles podem ser utilizados de forma legal e ética. Os crackers usam esse vírus pra ter acesso informações sigilosa por exemplo senhas, número dos cartões de crédito ou quaisquer informações pessoais.

Para se proteger contra *keyloggers* e outros *malwares*, é essencial adotar práticas de segurança digital, como manter o *software* e o sistema operacional atualizados, utilizar soluções de segurança confiáveis, evitar o download de programas de fontes não confiáveis e estar atento a e-mails, mensagens ou links suspeitos. Além disso, o uso de teclados virtuais ou *softwares* de criptografia de dados também pode ser uma medida preventiva eficaz contra *keyloggers*.

Figura 3- Ilustração hacker gravando as informações tecladas

Fonte: Autoria própria

Ransomware: é um tipo de *malware* (software malicioso) que criptografa os arquivos ou bloqueia o acesso a um sistema ou dispositivo, tornando os dados inacessíveis para o usuário. Os criminosos cibernéticos por trás do *ransomware* exigem então o pagamento de um resgate (*ransom*) em troca da chave de descriptografia ou da liberação do sistema.

Existem duas principais categorias de *ransomware*:

1. *Ransomware* de criptografia: Esse tipo de *ransomware* utiliza algoritmos de criptografia para tornar os arquivos do usuário ilegíveis. Os arquivos só podem ser descriptografados com uma chave específica, que é mantida pelos criminosos. Normalmente, uma mensagem é exibida na tela do dispositivo, informando à vítima que seus dados foram criptografados e exigindo um pagamento em criptomoedas ou outro meio anônimo para obter a chave de descriptografia.

2. *Ransomware* de bloqueio: Essa variante bloqueia o acesso ao dispositivo ou sistema, impedindo que o usuário utilize suas funções normais. Uma mensagem é exibida na tela, muitas vezes simulando ser de uma autoridade ou agência governamental, alegando que o usuário violou a lei e precisa pagar uma multa para desbloquear o dispositivo.

Figura 4- Representação ilustrativa *Ransomware*

Fonte: https://malware-guide.com/pt/como-retirar-bhui-ransomware-e-descriptografar-arquivos-bhui

Golpe do perfil falso no WhatsApp: é uma forma de fraude online em que um indivíduo cria uma conta falsa em redes sociais, aplicativos de mensagens ou outras plataformas digitais, fingindo ser outra pessoa ou representando uma identidade fictícia. O objetivo principal desse golpe é enganar os usuários, ganhar sua confiança e, eventualmente, obter benefícios financeiros ou informações pessoais das vítimas.

Nesse tipo de golpe, os golpistas geralmente criam perfis com fotos e informações de outras pessoas reais, copiando detalhes de seus perfis públicos ou roubando suas fotos. Eles podem usar nomes semelhantes ou fazer pequenas alterações nos nomes para evitar serem detectados facilmente.

Figura 5- Representação ilustrativa do golpe perfil falso do WhatsApp

Fonte: Autoria própria

Golpe do link falso: é uma tática de fraude online em que os golpistas enviam links maliciosos que se assemelham a sites legítimos, induzindo os usuários a clicarem neles. Esses links podem ser enviados por e-mail, mensagens de texto, redes sociais, aplicativos de mensagens instantâneas ou qualquer outra plataforma digital.

O principal objetivo do golpe do link falso é direcionar os usuários a páginas fraudulentas que buscam roubar informações pessoais, como senhas, dados bancários, números de cartões de crédito ou outras informações confidenciais. Essas páginas falsas são projetadas para se parecerem com sites autênticos, como bancos, lojas online, provedores de serviços ou plataformas populares, a fim de enganar os usuários e fazê-los fornecer suas informações confidenciais.

Os golpistas podem usar várias técnicas para disseminar os links falsos:

1. E-mails de *phishing*: Envio de e-mails que parecem ser de empresas ou instituições legítimas, contendo links que levam a páginas falsas.
2. Mensagens de texto: Envio de mensagens SMS ou aplicativos de mensagens com links falsos para induzir os usuários a clicarem neles.
3. Redes sociais: Publicação de links falsos em postagens, comentários ou mensagens privadas para atrair os usuários.
4. Sites comprometidos: Inserção de links falsos em sites comprometidos ou em anúncios maliciosos em sites legítimos.

Figura 6- Golpe do link falso

Fonte: Autoria própria

Golpe do boleto falso: O golpe de boletos falsos é uma prática criminosa que envolve a criação de boletos bancários falsificados, os quais são enviados às vítimas com o intuito de obter pagamentos indevidos. Esse tipo de golpe é amplamente utilizado para fraudar pagamentos diversos, como contas de serviços, boletos de compras online, mensalidades, taxas e outras despesas. Os golpistas, habilidosos em suas artimanhas, conseguem obter os dados necessários para criar os boletos falsos por meio de técnicas como engenharia social, phishing ou até mesmo através do roubo de informações de empresas e indivíduos desavisados. É comum que utilizem informações reais de empresas ou instituições financeiras, alterando apenas os dados do beneficiário ou do código de barras do boleto, dessa forma redirecionando o pagamento para suas próprias contas.

Quando as vítimas recebem e realizam o pagamento desses boletos falsos, o dinheiro é direcionado diretamente para as contas dos criminosos. O resultado é que a vítima acaba arcando com um prejuízo financeiro considerável, uma vez que a cobrança verdadeira permanece em aberto e ainda precisa ser quitada. É importante destacar a necessidade de estar sempre atento e cauteloso ao receber boletos e realizar pagamentos. Verificar cuidadosamente todos os detalhes do documento, como informações do beneficiário, código de barras e valor a ser pago, pode ajudar a evitar cair nesse tipo de golpe financeiro. Caso haja qualquer suspeita ou indício de fraude, é fundamental entrar em contato com a empresa ou instituição financeira responsável para confirmar a veracidade do boleto antes de efetuar o pagamento.

Golpe do PIX: é uma modalidade de fraude que se aproveita do sistema de pagamentos instantâneos implementado pelo Banco Central do Brasil. Nesse tipo de golpe, os criminosos utilizam técnicas avançadas de engenharia social com o objetivo de ludibriar as vítimas e obter dinheiro de forma indevida. Os golpistas se aproveitam da facilidade e rapidez do Pix para convencer as pessoas a realizarem transferências financeiras para contas fraudulentas. Eles podem se passar por representantes de empresas, instituições financeiras ou até mesmo amigos e familiares em situações de emergência, criando uma falsa sensação de urgência e necessidade imediata de pagamento.

Por meio de mensagens persuasivas, telefonemas ou até mesmo invadindo a privacidade das vítimas, os golpistas conseguem obter informações pessoais e bancárias que permitem realizar transações fraudulentas através do Pix. Eles podem solicitar códigos de autenticação, senhas ou até mesmo induzir as vítimas a escanear QR codes maliciosos que direcionam o pagamento para suas próprias contas.

Figura 7- Golpe do pix

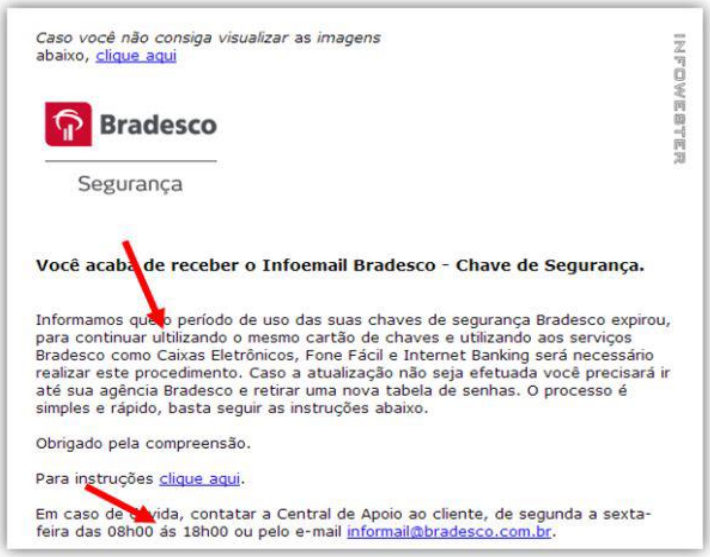
Fonte: https://bipbrasil.com.br/modernizacao-do-sistema-bancario-brasileiro-veja-cinco-tendencias-para-2021/

3.2 As principais formas de evitar golpes virtuais

***Phishing*:** para evitar cair em golpes de *phishing*, é essencial adotar algumas práticas de segurança digital, como:

- Verificar a legitimidade do remetente antes de clicar em links ou fornecer informações pessoais.
- Não responder a e-mails, mensagens ou telefonemas suspeitos que solicitam informações confidenciais.
- Utilizar autenticação de dois fatores sempre que possível para aumentar a segurança de contas online.
- Manter o software de segurança, navegadores e sistemas operacionais atualizados.
- Verificar a URL do site antes de inserir informações sensíveis. Certifique-se de que o site seja legítimo e seguro.

Figura 8 - Erros em um e-mail falso em nome de um banco



Fonte: https://www.infowester.com/phishing.php

***Trojan*:** quando um Trojan é executado no sistema da vítima, ele pode realizar diversas ações maliciosas, como:

1. Roubo de informações: Alguns Trojans são projetados para roubar informações confidenciais, como senhas, números de cartão de crédito e dados pessoais, e enviá-los para os hackers.
2. Controle remoto: Alguns Trojans podem abrir uma porta nos sistemas afetados, permitindo que os hackers acessem remotamente o dispositivo infectado, assumindo o controle completo.
3. Destruição de dados: Alguns Trojans são programados para apagar ou corromper dados importantes no dispositivo infectado.
4. Ataque a outros sistemas: Alguns Trojans são usados como ferramentas para lançar ataques a outros computadores ou redes, tornando o dispositivo da vítima parte de uma *botnet*.

Keylogger:

1. Mantenha seu sistema operacional e programas atualizados regularmente, pois as atualizações geralmente incluem correções de segurança importantes.

2. Utilize um software antivírus confiável e mantenha-o sempre atualizado para detectar e remover possíveis ameaças, incluindo *keyloggers*.
3. Evite clicar em links suspeitos ou baixar arquivos de fontes não confiáveis, pois eles podem conter *malware* que contém *keyloggers*.
4. Seja cauteloso ao inserir informações confidenciais, como senhas, em dispositivos públicos ou em computadores compartilhados, pois eles podem ter *keyloggers* instalados.
5. Considere o uso de autenticação de dois fatores sempre que possível, pois isso adiciona uma camada extra de segurança à sua conta.
6. Utilize senhas fortes e únicas para cada uma de suas contas online, evitando o uso de informações pessoais óbvias.
7. Fique atento a qualquer atividade suspeita em seu computador, como lentidão inexplicável ou comportamento estranho do sistema operacional, e realize verificações regulares em busca de malware.
8. Evite instalar software desconhecido ou de fontes não confiáveis em seu dispositivo, pois eles podem conter *keyloggers* ocultos.
9. Considere o uso de um teclado virtual ao inserir informações confidenciais em computadores públicos ou compartilhados, pois isso dificulta a captura de suas digitações por um *keylogger*.
10. Faça backups regulares de seus arquivos importantes, para que você possa recuperá-los caso seja vítima de um ataque de *keylogger*.

Ransomware: para se proteger contra o *ransomware*, é essencial adotar boas práticas de segurança digital, como manter o sistema operacional e o software atualizados, utilizar soluções de segurança confiáveis, evitar o download de arquivos de fontes não confiáveis e estar atento a e-mails ou mensagens suspeitos. Além disso, realizar backups regulares de seus dados em dispositivos externos ou na nuvem é uma medida importante para minimizar os danos causados por um ataque de *ransomware*.

Figura 9- Representação do golpe de *Ransomware*

Fonte:https://sisloc.com/blog/fique-atento-aos-golpe-do-boleto-falso/

Golpe do perfil falso no WhatsApp:

Uma vez que o perfil falso é criado, os golpistas podem agir de diferentes maneiras, tais como:

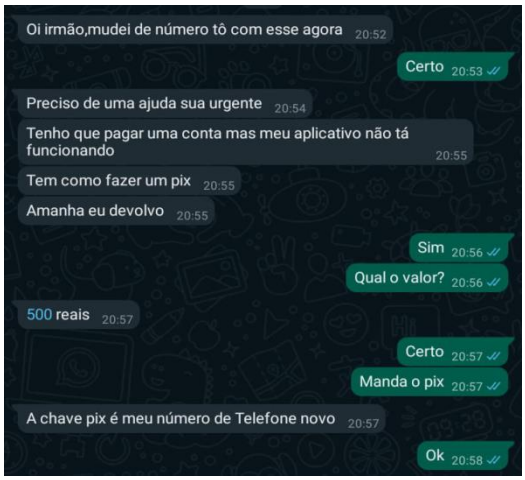
1. Enganar amigos ou conhecidos da pessoa real: Eles podem enviar mensagens ou solicitações de amizade para pessoas próximas à pessoa cuja identidade estão falsificando, buscando obter informações pessoais, como números de telefone, endereços ou outras informações confidenciais.

2. Espalhar desinformação ou conteúdo prejudicial: Os golpistas podem usar o perfil falso para disseminar informações falsas, propagar boatos, difamar a reputação de alguém ou promover conteúdo prejudicial ou ofensivo.

3. Enganar e extorquir outras pessoas: Usando o perfil falso, os golpistas podem entrar em contato com outras pessoas, fingindo ser a pessoa real, e tentar extorquir dinheiro ou informações confidenciais delas.

4. Realizar fraudes financeiras: Os golpistas podem utilizar o perfil falso para enganar pessoas e induzi-las a realizar transações financeiras fraudulentas, como investir em esquemas ilegítimos ou fazer doações para supostas causas de caridade

Figura 10 - Golpistas se passando por pessoa próxima a vítima



Fonte: Autoria própria

Golpe do link falso:

Para se proteger contra o golpe do link falso, é importante adotar algumas práticas de segurança digital:

- Verificar a URL do link antes de clicar para garantir que seja do site legítimo.

- Não clicar em links recebidos de fontes desconhecidas ou suspeitas.

- Evitar fornecer informações pessoais ou sensíveis em páginas cuja autenticidade não possa ser verificada.

- Utilizar softwares de segurança, como antivírus e firewall, para proteger o dispositivo contra ameaças online.

- Manter o sistema operacional, os navegadores e os aplicativos atualizados para corrigir possíveis vulnerabilidades de segurança.

Golpe do boleto falso:

Os golpistas podem usar várias técnicas para disseminar os links falsos:

1. E-mails de *phishing*: Envio de e-mails que parecem ser de empresas ou instituições legítimas, contendo links que levam a páginas falsas.

2. Mensagens de texto: Envio de mensagens SMS ou aplicativos de mensagens com links falsos para induzir os usuários a clicarem neles.
3. Redes sociais: Publicação de links falsos em postagens, comentários ou mensagens privadas para atrair os usuários.
4. Sites comprometidos: Inserção de links falsos em sites comprometidos ou em anúncios maliciosos em sites legítimos.

Golpe do PIX:

Para evitar cair no golpe do Pix, é importante seguir algumas medidas de segurança.

- Sempre verifique as informações do recebedor antes de realizar um Pix, especialmente se você não tiver realizado transações com essa pessoa ou empresa anteriormente.

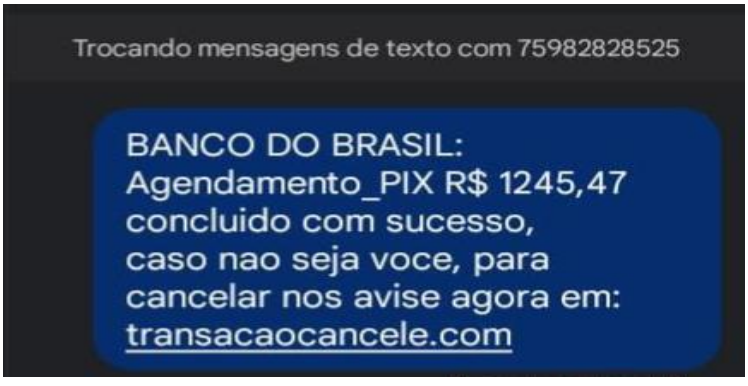
- Nunca compartilhe suas informações de chaves Pix ou *QRcode* com fontes desconhecidas ou suspeitas.

- Desconfie de ligações, mensagens ou e-mails que solicitem Pix para situações não esperadas ou sem confirmação prévia.

- Utilize sempre canais oficiais de contato para verificar informações ou realizar transações financeiras.

- Se receber solicitações suspeitas, entre em contato diretamente com a instituição financeira ou empresa envolvida para confirmar a veracidade da solicitação.

Figura 11- Mensagem falsa golpe do Pix



Fonte: Autoria própria

4.0 PRODUTO: CRIAR UM SITE ORIENTANDO SOBRE FORMAS DE EVITAR GOLPES VIRTUAIS, UTILIZANDO A PLATAFORMA DA HOSTINGER.

Este projeto visa fornecer uma plataforma abrangente e acessível que capacita os usuários a navegar pela internet com confiança e segurança. O site que estamos desenvolvendo tem como objetivo central oferecer informações valiosas, dicas práticas e orientações claras para prevenir uma série de golpes cibernéticos que têm se tornado cada vez mais comuns nos dias de hoje.

Aqui está uma visão geral das áreas que nosso site irá abordar:

1. Educação sobre Golpes Cibernéticos:

Vamos criar seções dedicadas a diferentes tipos de golpes cibernéticos, explicando como eles funcionam, quais são os sinais de alerta e como evitá-los. Abordaremos golpes comuns, como *phishing*, *ransomware*, *keyloggers* e outros, detalhando as táticas que os criminosos usam para enganar os usuários.

2. Dicas de Segurança Online:

Iremos fornecer uma série de dicas práticas para ajudar os usuários a manterem-se seguros durante suas atividades online. Isso incluirá orientações sobre como criar senhas seguras, verificar a autenticidade de links e e-mails, manter o software atualizado e proteger informações pessoais.

3. Exemplos e Estudos de Caso:

Faremos uso de exemplos reais e estudos de caso para ilustrar como os golpes cibernéticos podem ocorrer na vida real. Isso ajudará os usuários a identificar padrões suspeitos e tomar medidas proativas para evitar serem vítimas.

4. Perguntas Frequentes e Suporte:

Criaremos uma seção de perguntas frequentes que abordará dúvidas comuns dos usuários. Além disso, ofereceremos opções de suporte para quem precisar de assistência adicional ou tiver dúvidas específicas sobre segurança cibernética.

O objetivo final deste site é empoderar os usuários com o conhecimento e as ferramentas necessárias para se protegerem contra golpes cibernéticos. Acreditamos que, ao fornecer informações claras e acessíveis, podemos ajudar a reduzir o impacto desses crimes e criar um ambiente online mais seguro para todos.

O que é a *Hostinger*?

A *Hostinger* é uma plataforma de hospedagem amplamente reconhecida que oferece uma gama de serviços para criar e hospedar sites com facilidade e eficiência. Sua confiabilidade e vantagens em relação à criação manual de código atraem tanto iniciantes quanto profissionais da web. Aqui está um texto explicando por que a plataforma da *Hostinger* é uma escolha sólida em comparação à construção manual de um site. A plataforma Hostinger oferece uma solução confiável e eficaz para criar e hospedar sites. Sua confiabilidade é respaldada por avaliações positivas e baixas taxas de tempo de inatividade. Com uma interface amigável, ela simplifica a criação de sites, eliminando a necessidade de habilidades técnicas avançadas. A plataforma também economiza tempo e esforço, fornecendo recursos pré-construídos, como modelos e plugins. Além disso, o suporte técnico especializado garante assistência desde a configuração até a manutenção contínua. A *Hostinger* oferece uma alternativa prática e eficiente à construção manual de código, adequada para todos, desde iniciantes até profissionais da web.

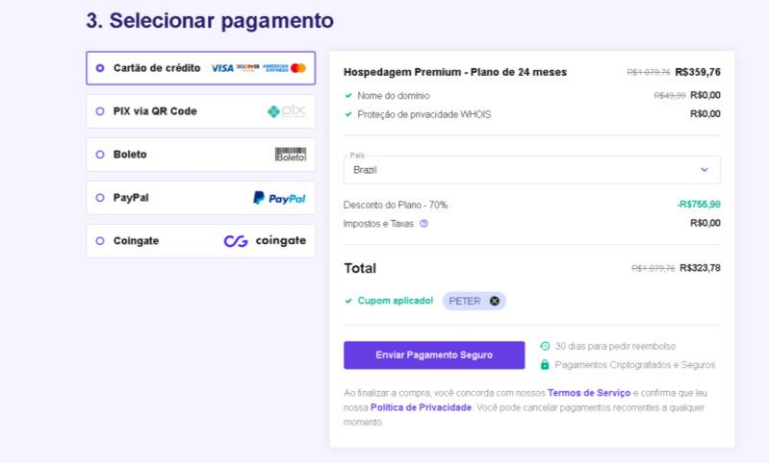
Figura 12- Logo da *Hostinger*

Fonte: https://www.hostinger.com/

4.1 Construção do Site

- O primeiro passo consistiu na elaboração de um plano de dois anos, com um pagamento total de 323,78 reais, resultando na aquisição do plano Premium de hospedagem web.

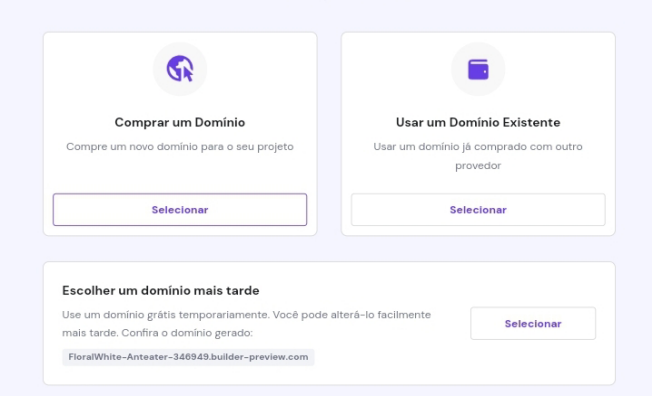
Figura 13- Criação de Plano na *Hostinger*



Fonte: https://cart.hostinger.com/pay/

- No segundo passo, no âmbito da plataforma de hospedagem, procedemos à criação de um domínio denominado "*Digital Protection Against Virtual Scams*" (DPAVS).

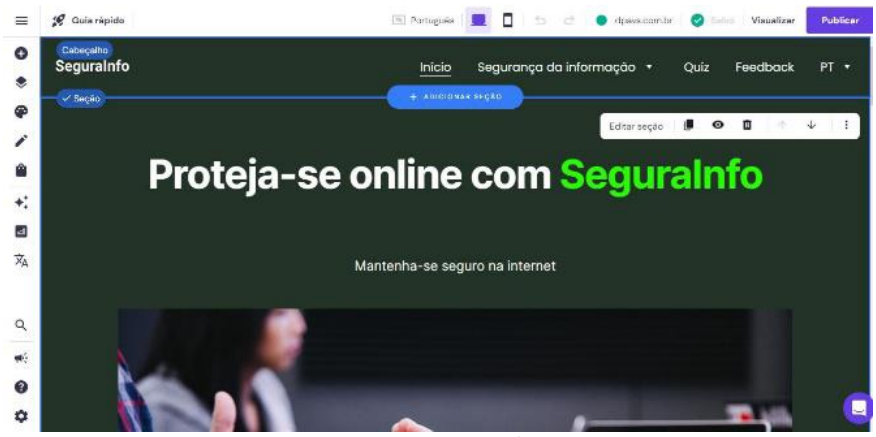
Figura 14- Criação de domínio na *Hostinger*



Fonte: https://hpanel.hostinger.com/

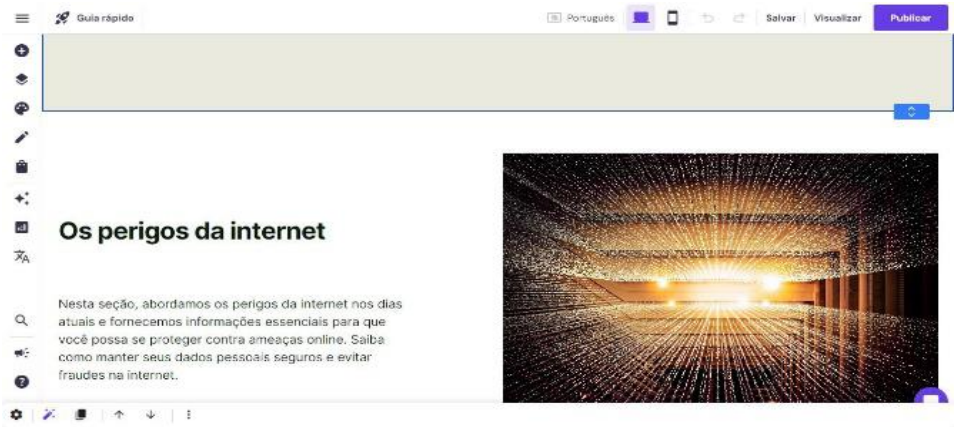
- No terceiro passo, concebi a página inicial da web site, apresentando uma dissertação acerca do tópico da segurança da informação, explicitando a finalidade do web site. Adicionalmente, esta página contém caixas que proporcionam o acesso às secções de questionários, feedback e explicações sobre golpes.

Figura 15- Inicio pagina



Fonte: SeguraInfo

Figura 16 - Página com os Perigos da Internet



Fonte: SeguraInfo

- O quarto passo envolveu a criação das páginas relativas aos diferentes tipos de golpes virtuais. malwares Segurança da informação. Para preenchimento

de tais páginas, foram utilizados os materiais investigados na fase de "pesquisa e análise dos principais golpes comuns na internet".

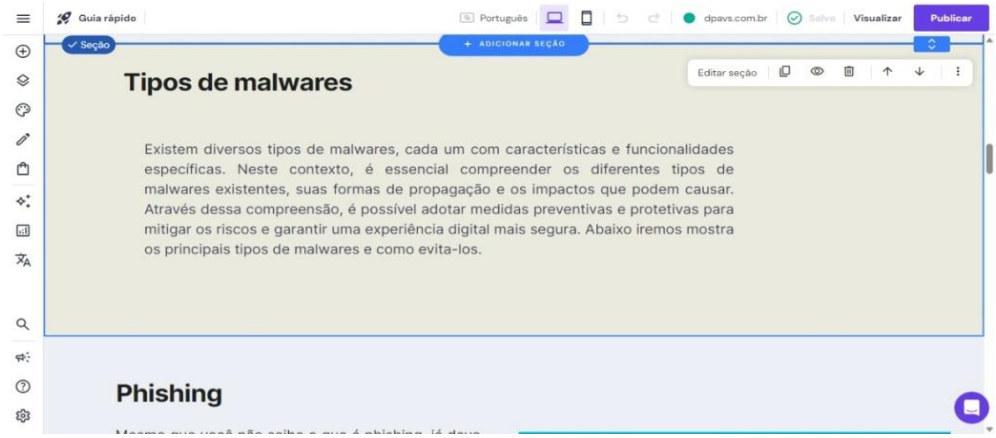
Figura 17- Página de Golpes virtuais

Fonte: SeguraInfo

Figura 18 - Página de Malwares

Fonte: SeguraInfo

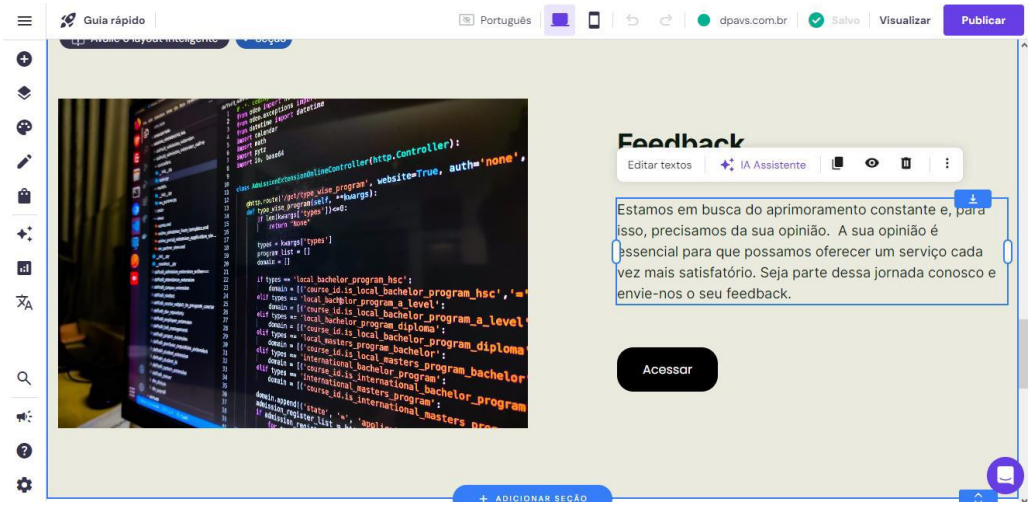
Figura 19- Página Tipos de Malwares



Fonte: SeguraInfo

- No quinto passo, desenvolveu-se a página de feedback, contendo um questionário que solicita a opinião dos utilizadores, juntamente com os seus nomes e endereços de e-mail. Importa salientar que este feedback será remetido ao endereço de e-mail dpavsassist@gmail.com.

Figura 20 - Caixa de feedback



Fonte: SeguraInfo

- No sexto passo, implementou-se uma página que orienta os utilizadores para completarem os três questionários abordando os temas dos malwares, segurança da informação e diferentes tipos de golpes.

Figura 21- Pagina de quiz

Fonte: SeguraInfo

- No sétimo passo, foram criadas três páginas de questionários, cada uma contendo um total de doze questões, à exceção do questionário sobre segurança da informação, que abarca cinco questões.

Figura 22- Quiz de malwares

Fonte: SeguraInfo

Este foi o passo a passo de criação do produto proposto, valendo ressaltar que trata-se apenas de um resumo, limitando-se à amostra do desenvolvimento visual do site. Pôde-se observar que o site foi desenvolvido com o intuito de educacional, ou seja, para orientar o leitor em relação a prevenção contra golpes virtuais.

5.0 Conclusão

O desenvolvimento deste trabalho permitiu tomar noção da vasta quantidade de golpes virtuais presentes no ambiente digital, que se destacam principalmente pelo fato de serem altamente planejados e bem executados. Essa modalidade utiliza principalmente da manipulação de pessoas ingênuas ou que muitas vezes sofrem com a falta de conhecimento em relação a quais dados elas devem ou não fornecer aos serviços que elas utilizam. Ao decorrer desta pesquisa foram apresentados vários tipos de golpes, sendo eles por exemplo o *phishing* ou até mesmo os golpes de *ransomware*. O *phishing* é um tipo de golpe que tem como objetivo obter informações confidenciais como senhas, números de cartão de crédito e informações bancárias, através do envio de mensagens falsas ou sites fraudulentos. Já o *ransomware* é um tipo de *malware* que sequestra informações do usuário e exige uma quantia em dinheiro para liberá-las.

A exposição desses tipos de golpes e outros durante a pesquisa evidenciou a importância da segurança da informação, sendo que no ambiente digital é ainda mais difícil de mantê-la. Em muitos casos, os golpistas utilizam técnicas sofisticadas para enganar as vítimas, tornando difícil a identificação da ameaça.

Por esse motivo, é imprescindível adotar medidas preventivas para evitar ser vítima desses golpes virtuais. Durante a pesquisa, foram encontradas diversas formas de prevenção, como usar softwares antivírus atualizados e confiáveis, manter o sistema operacional e programas sempre atualizados, evitar clicar em links suspeitos ou baixar arquivos de fontes não confiáveis e utilizar senhas fortes e únicas para cada uma das contas online. Além disso, é importante estar atento à atividade suspeita no computador ou dispositivo móvel, como lentidão inexplicável ou comportamento estranho do sistema operacional. Realizar verificações regulares em busca de malware também é fundamental para garantir a segurança da informação. Outra medida preventiva importante é adotar a autenticação de dois fatores sempre que possível. Essa medida acrescenta uma camada extra de segurança à conta e dificulta ainda mais o acesso indevido por parte dos golpistas.

Ficou evidente na pesquisa que a educação digital é fundamental para prevenir os golpes virtuais. É importante disseminar informações sobre as ameaças digitais e sobre as melhores práticas para evitar ser vítima desses golpes. Dessa forma, será possível criar uma cultura mais segura na internet. Portanto, todas as formas de prevenção encontradas durante o decorrer da pesquisa mesmo que não tenham sido testadas efetivamente, mostram-se extremamente funcionais e confiáveis na proteção dos usuários. É imprescindível adotar práticas seguras e estar constantemente atualizado sobre as ameaças digitais para preservar a integridade das informações.

Ao criar um site pela plataforma da Hostinger apresentou algumas dificuldades. A plataforma da Hostinger exige certa familiaridade com conceitos técnicos, como registro de domínio, configuração de DNS, conhecimento básico de html e gerenciamento de servidores. Além disso, a personalização do site pode ser limitada pelas opções oferecidas pela plataforma, requerendo conhecimentos avançados de programação para implementar recursos personalizados. No entanto, com paciência, pesquisa e disposição para aprender, foi possível superar esses obstáculos e criar um site funcional e atraente na plataforma da Hostinger.

7.0 REFERENCIAS

PRODEST. **Entenda o que é phishing e adote medidas para evitá-lo** Cidade : Av. João Batista Parra, 465 - Praia do Suá . 2015 -2023 Disponível em : https://prodest.es.gov.br/entenda-o-que-e-phishing-e-adote-medidas-para-evita-lo

SANTOS , sérgio .FERREIRA , André.**Prevenção a golpes Virtuais e presenciais** Cidade : Santo Antônio, Recife, PE . 2021 Disponível em : https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2022/02/prevencao-a-golpes-virtuais-e-presenciais.pdf

MARCIANO , João Luiz .MARQUES , mamede. **O enfoque social da segurança da informação** cidade : Brasília, 16 de março de 2007 Disponível em: https://www.scielo.br/j/ci/a/L8CqcznptmQK3jyqGqNpWMQ/abstract/?lang=pt

NIC.BR . NUCLEO DE INFORMACAO E COORDENACAO DO PONTO BR **Cartilha de Seguranca para Internet ,** cidade : Sao Paulo 2012 . Disponível em : https://www.100security.com.br/downloads/conscientizacao/cartilha-seguranca-na-Internet.pdf

KLEIN , Esther .TREULIEB ,Luciane .Dias ,Maurício . **Como se proteger de golpes na internet** cidade : Santa Maria - RS . 28 de julho de 2021 . Disponível em : https://www.ufsm.br/midias/arco/como-se-proteger-de-golpes-na-internet

OSTEC. **Trojan: saiba tudo sobre esse malware e como se proteger dele** Cidade: Rua Coronel Cabral, 158, Centro - Tubarão . 19 de fevereiro de 2020 Disponível em : https://ostec.blog/geral/trojan/

ROSENBAUM, guinsburg . **Proteja-se dos 7 golpes mais comuns da internet** Cidade : Avenida Paulista, São Paulo – SP 24 de março de 2023 . Disponível em : https://www.rosenbaum.adv.br/proteja-se-dos-principais-7-golpes-internet/

SISLOC . **SislocFique atento ao golpe do Boleto Falso** - 2023 Disponível em :https://sisloc.com/blog/fique-atento-aos-golpe-do-boleto-falso/

BELCIC , Ivan . **O que e senha forte ?** Publicado em 23 de setenbro de 2021 . Disponivel em : https:www.avg.com/PT/sinal/how-to-create-a-stong-password-that-you-wontf

SOFTSYSTEM.**Vírus ransomware** cidade:Lago Sul Brasília - DF 19 junho 2023 disponível em : https://www.softsystem.com/softsystem/exibeNoticias.jsp?publicacao.codPublicacao=1036&codListaTipoPublicacao=2

FIA . **Segurança da informação: o que é, 5 pilares e como garantir nas empresas?** Cidade : São Paulo - SP . Disponível em :https://fia.com.br/blog/seguranca-da-informacao/

PREUSS , marcos . **Aprenda sobre *malware* e como proteger todos os seus dispositivos contra eles** - 2023 DISPONIVEL EM : https://kaspersky.com.br/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

SILVA .denise . STEIM ,Lilian . **Segurança da informação ; uma reflexão sobre o componente humano.** Cidade: Rio Grande do Sul . Publicado em 31 de marco de 2007. Disponivel em : http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=s1806-58212007000100006

Link de tabela 1 - Nível de Segurança das Senhas :https://www.hivesystems.io/blog/are-your-passwords-in-the-green