PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

ENGENHARIA SOCIAL: ESTUDO DE ATAQUES E MÉTODOS DE PREVENÇÃO

LEONARDO DE MOURA ALVES

GOIÂNIA
2024

LEONARDO DE MOURA ALVES

ENGENHARIA SOCIAL: ESTUDO DE ATAQUES E MÉTODOS DE PREVENÇÃO

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação.
Orientador:
Profa. Dra. Solange da Silva
Banca examinadora:
Prof. Me. Fernando Gonçalves Abadia
Prof. Me. Rafael Leal Martins

GOIÂNIA

2024

LEONARDO DE MOURA ALVES

ENGENHARIA SOCIAL: ESTUDO DE ATAQUES E MÉTODOS DE PREVENÇÃO

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Ciência da computação, em 20/06/2024.

Orientadora: Profa. Dra. Solange da Silva

Prof. Me. Fernando Gonçalves Abadia

Prof. Me. Rafael Leal Martins

GOIÂNIA

2024

AGRADECIMENTOS

Quero agradecer primeiramente a Deus que me deu força para continuar mesmo nos momentos difíceis da minha vida.

Agradeço a minha madrinha, mãe e pai que foram os pilares da minha vida, me apoiaram nas minhas escolhas e sempre me incentivaram com a minha graduação.

Em memórias a minha avó materna, que nos deixou no ano de 2023, que sempre me inspirou, me aconselhou sobre o futuro e minha avó paterna que me apoia orienta.

Agradeço à minha orientadora Doutora Solange da Silva pelo interesse, dedicação, paciência, consolo nos momentos difíceis e orientação neste TCC.

Agradeço a Central Sicoob UNI e meu colegas da equipe de Tecnologia da informação pelo aprendizado, amizade e apoio.

Agradeço aos professores e a PUCGO por me proporcionar o conhecimento necessário para contribuir com meu desenvolvimento.

RESUMO

O objetivo deste trabalho é informar os principais ataques de engenharia social na computação, como é realizado os ataques, exemplos reais de ataques e como se prevenir. Quantos aos aspectos metodológicos é uma pesquisa bibliográfica e experimental. O estudo permitiu concluir que há diversos tipos de ataques de engenharia social, tais como, *pshising*, *baiting*, *tailgating*, *scareware*, *watering hole*, *quid pro quo*, *open source intelligence* e *dumpster divind*. Na medida em que a tecnologia avança, os ataques de engenharia social tornam-se cada vez mais frequentes. Portanto, é essencial intensificar os esforços na prevenção e conscientização dos usuários sobre essas ameaças, visto que podem causar danos irreversíveis e inimagináveis. Com a tecnologia cada vez mais presente no dia a dia da população deve-se adotar medidas de segurança para proteção própria. Muitas das falhas sistemáticas se dão ao erro humano, que pode gerar inúmeras consequências. A conscientização da possibilidade de uma invasão através dos métodos de engenharia social mostra-se essencial para fortalecer o ambiente cibernético e a proteção de dados.

Palavra chaves: Engenharia Social. Ataques Cibernéticos. Segurança da Informação. Prevenção de Fraudes. Fraudes Cibernéticas.

ABSTRACT

The objective of this work is to inform the main social engineering attacks in computing, how attacks are carried out, real examples of attacks and how to prevent them. As for the methodological aspects, it is a bibliographic and experimental research. The study concluded that there are several types of social engineering attacks, such as pshising, baiting, tailgating, scareware, watering hole, quid pro quo, open source intelligence and dumpster divind. As technology advances, social engineering attacks become increasingly frequent. Therefore, it is essential to intensify efforts to prevent and raise awareness among users about these threats, as they can cause irreversible and unimaginable damage. With technology increasingly present in the population's daily lives, security measures must be adopted to protect themselves. Many of the systematic failures are due to human error, which can generate countless consequences. Awareness of the possibility of an invasion through social engineering methods is essential to strengthen the cyber environment and data protection.

Keywords: Social Engineering. Security. Cybernetics.

Keywords: Social Engineering. Cyber Attacks. Information security. Fraud Prevention. Cyber Fraud.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS E ABREVIATURAS

2FA	*Two-Factor Authentication* ou Autenticação de Dois Fatores
CEO	*Chief Executive Officer* ou Diretor Executivo
CERT.BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CMS	*Content Management System* ou Sistema de Gerenciamento de Conteúdo
CNN	*Cable News Network*
CPF	Cadastro de Pessoas Físicas
CPU	*Central Processing Unit* ou Unidade Central de Processamento
CSM	*Continuous Security Monitoring* ou Monitoramento Contínuo de Segurança
DDoS	*Distributed Denial of Service* ou Negação de serviço distribuída
DKIM	*DomainKeys Identified Mail* ou Correio Identificado por Chaves de Domínio
DLP	*Data Loss Prevention* ou Prevenção de Perda de Dados
DMARC	*Domain-based Message Authentication, Reporting, and Conformance* ou Autenticação de Mensagens, Relatórios e Conformidade Baseada em Domínio
DNS	*Domain Name System* ou Sistema de Nomes de Domínio
DVD	*Digital Versatile Disc* ou Disco Óptico Digital
E-MAIL	*Messages electronically* ou Correio Eletrônico
EOP	*Exchange Online Protection ou* Proteção Online do *Exchange*
HD	*Hard Disk ou Disco Rígido*
HTML	*HyperText Markup Language* ou Linguagem de Marcação de Hipertexto
IA	*Artificial Intelligence* ou Inteligência Artificial
IBM	*International Business Machines Corporation*
IDS	*Intrusion Detection System* ou Sistema de Detecção de Intrusões
IPS	*Intrusion Prevention System* ou Sistema de Prevenção de Intrusões
LGPD	Lei Geral de Proteção de Dados Pessoais

OSINT	*Open Source Intelligence* ou Inteligência de Fonte Aberta
PIX	Sistema de Pagamento Instantâneo Brasileiro
PUCGO	Pontifícia Universidade Católica de Goiás
RG	Registro Geral
SMS	*Short Message Service* ou Serviço de Mensagem Curta
SPF	*Sender Policy Framework* ou Estrutura de Política do Remetente
SSD	*Solid-State Drive* ou Unidade de Estado Sólido
TCC	Trabalho de Conclusão de Curso
TI	Tecnologia da Informação
URL	*Uniform Resource Locator* ou Localizador Uniforme de Recursos
USB	*Universal Serial Bus* ou Porta Serial Universal

SUMÁRIO

1 INTRODUÇÃO

Segundo Fernandes (2023), a engenharia social é uma forma de ataque cibernético que explora a psicologia humana para obter acesso a informações sensíveis, sistemas ou redes. Ao invés de explorar vulnerabilidades técnicas, os criminosos cibernéticos exploram as fraquezas humanas, manipulando as vítimas para divulgar informações confidenciais, clicar em *links* maliciosos ou executar ações prejudiciais.

O ser humano é considerado o elo mais vulnerável em qualquer sistema de segurança da informação, assim sendo um grande desafio para os profissionais de segurança, manter um ambiente cibernético seguro, pois a cada dia os invasores planejam novos métodos de persuadir e invasão aos sistemas (Rubinsteinn, 2020).

A possibilidade de uma invasão que possa comprometer a privacidade e a integridade mental de uma pessoa ou os sistemas de informação de uma empresa, podem parecer impossíveis até que se concretize. Para se prevenir esta realidade deve-se promover conscientização, educação, medidas protetivas nos ativos de informação, pois se trata de um risco real para qualquer sistema que envolva seres humanos (Mitnick, 2003).

“O Brasil teve um crescimento significativo no número de detecções de ataques de engenharia social no ano passado. Segundo a Eset, desenvolvedora de soluções de cibersegurança, houve aumento de pouco mais de 200% em 2020, comparado com o ano anterior, sendo agosto o mês com maior número de detecções.” (Febraban Tech, 2021).

“De acordo com o levantamento realizado por pesquisadores da companhia, o Brasil foi o segundo país da América Latina com maior incidência desse tipo de ataque, com 18% do total, atrás apenas do Peru, que registrou pouco mais de 31%. Outro país com alto índice é o México, que teve quase 17% das detecções na região.” (Febraban Tech, 2021).

Justifica estudar este tema pois, de acordo com Fernandes (2023), A Engenharia Social é uma ameaça persistente e em constante evolução que tem um impacto global significativo. Os criminosos cibernéticos continuam aperfeiçoando suas táticas de manipulação psicológica para explorar a ingenuidade e confiança das vítimas. Portanto, é crucial que indivíduos e organizações estejam cientes dos perigos

da Engenharia Social e adotem várias camadas de proteção para garantir a segurança de informações confidenciais e sistemas críticos. A conscientização, a educação e a implementação de práticas de segurança robustas são fundamentais para mitigar os riscos e fortalecer a resiliência contra essa forma de ataque cibernético.

Diante deste contexto, esse projeto visa responder a seguinte questão de pesquisa: - **Quais são os tipos de ataques de engenharia social na computação e como se proteger?**

O objetivo geral é realizar uma revisão bibliográfica para **identificar quais são os tipos de ataques cibernéticos de engenharia social e formas de prevenção.**

Os objetivos específicos são:

- Analisar as formas que são realizados os crimes cibernéticos utilizando engenharia social.
- Descrever os métodos de prevenção aos crimes cibernéticos de engenharia social

Espera-se que os resultados deste trabalho possam contribuir:

- Alertando os usuários sobre os tipos de ataques cibernéticos utilizando engenharia social
- Informando e conscientizando sobre a importância da segurança dos dados
- Mostrando a importância de se ter políticas de segurança de dados em uma empresa.
- Apresentando soluções para usuários e empresa para minimizar o risco de ataques de engenharia social

Esta monografia está estruturada da seguinte maneira, no capítulo 1 é introduzido o tema do trabalho, a questão de pesquisa, objetivo e resultados esperados. O capítulo 2 traz o referencial teórico com conceitos, definições, e trabalhos relacionados com o tema. No capítulo 3 é descrito o método, ou seja, como o trabalho foi desenvolvido e o que foi feito para que o objetivo geral fosse atingido. No capítulo 4 é mostrado os tipos de ataques de engenharia social, como os atacantes utilizam as ferramentas para manipular os ataques e exemplos de ataques. O capítulo 5 apresenta os métodos de prevenção e proteção aos ataques de engenharia social para usuários e empresas. O capítulo 6 traz as considerações finais e sugestões de trabalhos futuros.

2 REFERENCIAL TEÓRICO

Este capítulo é composto por conceitos e definições e sobre trabalhos relacionados.

2.1 CONCEITOS E DEFINIÇÕES

“Engenharia social é qualquer ataque que se aproveita da psicologia humana para influenciar um alvo, fazendo-os executar uma ação ou fornecer algumas informações” (Gray, 2021, p.3).

Os métodos de engenharia social têm como base a compreensão fundamentada na ciência da motivação humana. As vítimas têm suas emoções e instintos manipulados, levando a tomar decisões que não são dos seus melhores interesses (IBM, 2023).

> Influência é um termo neutro para direcionar o comportamento de uma pessoa para causar um resultado específico. A influência pode ser positiva ou negativa. A manipulação é uma implementação prejudicial de influência, normalmente destinada a causar danos. Na engenharia social, tanto maus atores quanto pessoas bem-intencionadas costumam usar a manipulação em vez de influência, seja por falta de formação ou por miopia (Gray, 2021, p.8).

2.2 SEGURANÇA CIBERNÉTICA

“A segurança cibernética é a prática de proteger computadores, redes, aplicações de *software*, sistemas essenciais e dados de possíveis ameaças digitais.” (Amazon, 2023). Todas as organizações têm a responsabilidade de preservar e proteger dados do cliente, conforme solicitado na Lei Geral de Proteção de Dados Pessoais, por isso, as empresas utilizam de técnicas de segurança e ferramentas para este controle da sua segurança cibernética.

“Em 2020, um estudo mostrou que o custo médio de uma violação de dados foi de USD 3,86 milhões em todo o mundo, e de USD 8,64 milhões nos Estados Unidos.” (IBM, 2023). Todos os anos empresas investem milhões para a proteção cibernética.

Empresas de todo mundo adotam práticas de segurança para minimizar o risco de invasões. Uma das principais táticas adotadas são, “segurança de confiança zero”, trata-se de não confiar em nem uma solicitação de acesso, mesmo vindo de uma rede

interna, assim limitando o acesso aos privilégios, concedendo ao empregado privilégios mínimos (Microsoft, 2023).

Outra estratégia adotada é treinamentos regulares de segurança cibernética. A segurança cibernética de uma empresa não é apenas responsabilidade dos profissionais de segurança, mas também dos empregados. Visando evitar ataques como *phishing* entre outros, empresas investem em treinamento para conscientizar e capacitar seus funcionários (Microsoft, 2023). Segundo Cryptoid (2023), o fator humano é primordial na defesa cibernética, mas as pessoas podem ser o elo mais forte se investirmos em capacitação, treinamentos e conscientização. Para reduzir risco de segurança cibernética, é estabelecido processo de prevenção, detecção e resposta a ataques, a prática leva à aquisição de ferramentas como antivírus e planos de contingência caso ocorra algum ataque.

2.3 ATAQUES CIBERNÉTICOS

O ataque cibernético tem como objetivo causar danos ou obter controle ou acessos a um sistema, os ataques podem ter tanto computadores pessoais ou empresas como alvos (Microsoft, 2023). Existem diversos ataques cibernéticos, mas o que não necessita de conhecimento técnico em computação são os ataques de *phishing*.

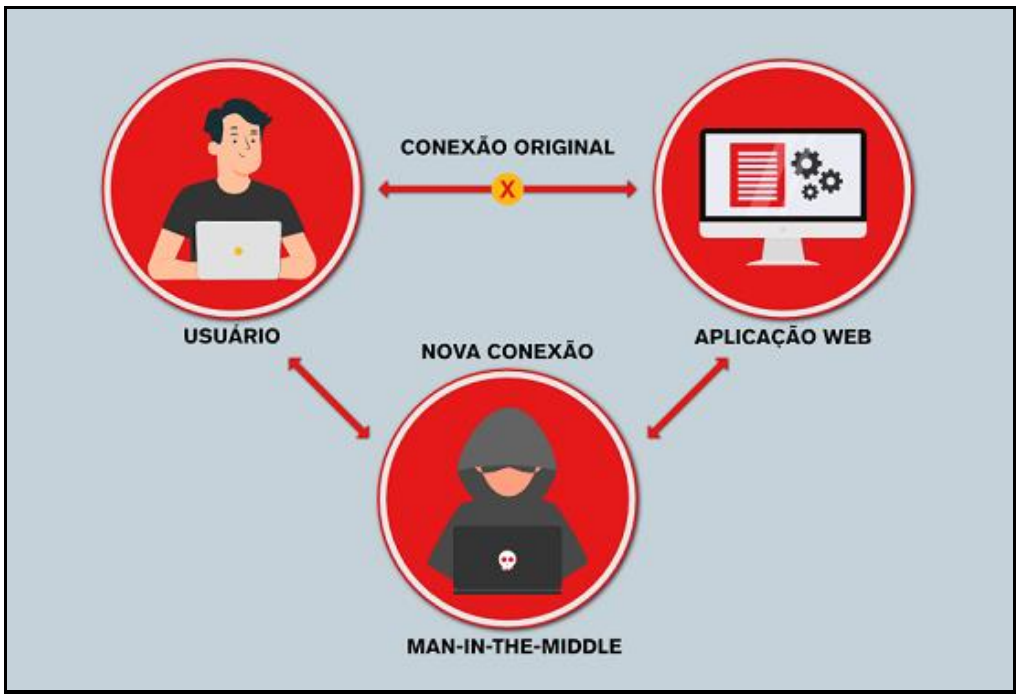
Os ataques de *malware* são *softwares* mal-intencionado, que são criados para passar uma imagem de confiança para os usuários, os criminosos fingem ser empresas reais e induzem o usuário a executar o *malware*, após a execução do *software*, o computador da vítima já se encontra infectado pelo vírus, assim dando vários benefícios ao atacante, como, coleta de dados, utilizam do poder do CPU da máquina, controle de dados, controle remoto da máquina, entre outros (Microsoft, 2023).

“*Ransomware* é um tipo de *software* mal-intencionado, ou *malware*, que ameaça uma vítima destruindo e bloqueando o acesso a dados críticos ou sistemas até que um resgate seja pago.” (Microsoft, 2023). O *ransomware* é um ataque mais voltado às empresas, o invasor após conseguir controle das máquinas da rede, ele utiliza de ferramentas de criptografia para criptografar todos os dados encontrados na rede e pedir um valor para resgatar os dados.

“Um ataque *man-in-the-middle* envolve uma parte externa que tenta obter acesso não autorizado por uma rede durante uma troca de dados. Esses ataques aumentam os riscos de segurança de informações sigilosas, como dados financeiros.” (Amazon, 2023).

“O invasor se posiciona entre duas partes que tentam comunicar-se, intercepta mensagens enviadas e depois se passa por uma das partes envolvidas.” (Malenkovich, 2013). Conforme mostrado na Figura 1, consegue-se visualizar como ocorre o ataque.

Figura 1 – Ilustração de um ataque *man-in-the-middle*



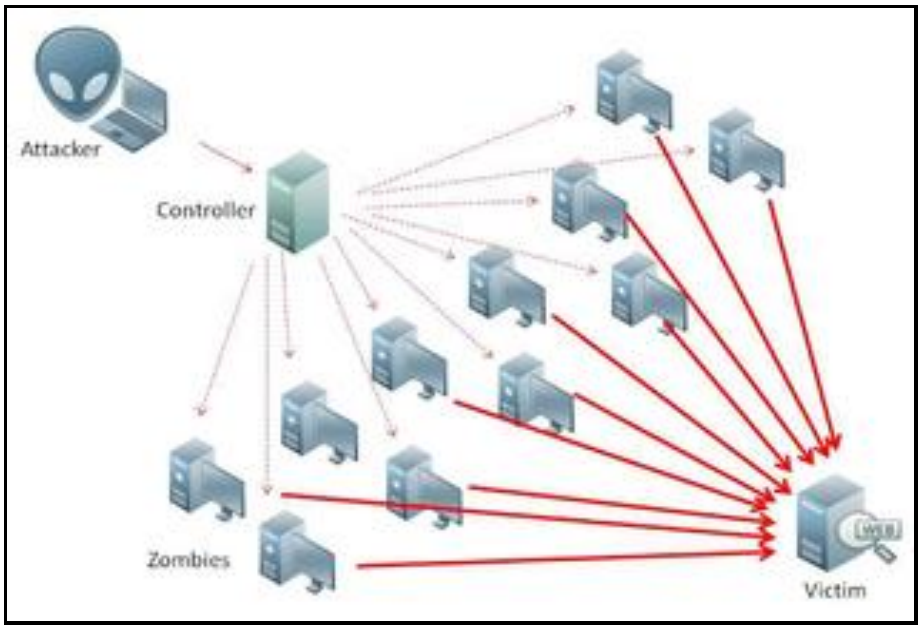
Fonte: Claranet, 2023.

No caso do exemplo da Figura 1, o criminoso está no meio da comunicação entre usuário e a aplicação web, isso permite que o criminoso possa ler as requisições que o usuário envia para a aplicação e alterá-las. Ele pode ler as respostas da aplicação web e realizar alterações.

“O *Distributed Denial of Service* (DDoS) ou ataque distribuído de negação de serviço é um esforço coordenado para sobrecarregar um servidor enviando um grande volume de solicitações falsas. Esses eventos impedem usuários normais de se conectar ou acessar o servidor de destino.” (Amazon, 2023).

Neste ataque o atacante tem como objetivo indisponibilizar um serviço ou aplicação, utilizando um sistema coordenado por *botnets*. Os *botnets* são uma rede de dispositivos comprometidos controlados pelo invasor, através desta rede, o atacante inicia uma sobrecarga dos recursos do servidor, fazendo com que o servidor que hospeda o serviço ou aplicação fique congestionado, levando à sua queda. É possível visualizar este ataque através da Figura 2,

Figura 2 – Ilustração de um ataque DDoS



Fonte: Wikipedia, 2022.

Na Figura 2, é possível observar o ataque, no qual a *Controller* ou mestre solicita aos *botsnets* ou *Zombies* que realizem uma série de solicitações à vítima.

2.4 LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Conforme a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.853, de 8 de Julho de 2019), o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

De acordo com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.853, de 8 de Julho de 2019), foi criada para proteger os direitos fundamentais de liberdade e

de privacidade, e a livre formação da personalidade de cada indivíduo. A Lei tem como objetivo o tratamento de dados feito por pessoa física ou jurídica de direito público ou privado.

A lei geral de proteção de dados tem o fundamento de respeito à privacidade, autodeterminação informativa, liberdade de expressão, de informação, de comunicação e de opinião, inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Com a criação da LGPD, tanto âmbito jurídico e física tem a obrigação de tratar os dados coletados com responsabilidade e respeito, tendo em vista a obrigação legal de proteger as informações e não as usar de forma inadequada.

2.5 TRABALHOS RELACIONADOS

Esta seção apresenta alguns trabalhos relacionados ao tema em estudo.

2.5.1 ENGENHARIA SOCIAL: ESTUDO DE CASO SOBRE OS RISCOS DE UM ATAQUE EFETUADO POR UM EX-FUNCIONÁRIO

Conforme apresentado por Meier (2018), foi apresentado a importância que as empresas devem ter em relação a engenharia social dentro do ambiente empresarial. O autor analisou os principais métodos utilizados, falhas humanas em relação à segurança cibernética e as consequências de um ataque.

O objetivo do trabalho foi demonstrar os riscos de um ataque cibernético efetuado por um ex-funcionário, métodos de prevenção e forma de execução do ataque.

No trabalho foi concluído que há necessidade de conscientizar pessoas e colaboradores em relação aos riscos da engenharia social no ambiente corporativo, demonstrando que os ataques poderiam ser evitados se a empresa se aplicadas boas práticas de segurança da informação.

3 MÉTODO

Esta pesquisa, segundo sua natureza, é um resumo de assunto, buscando elucidar a esfera de conhecimento do projeto ao destacar sua evolução histórica. Como resultado da investigação das informações obtidas na pesquisa, levando a conclusão do entendimento de suas causas e explicações (Wazlawic, 2014).

Quanto aos objetivos, esta pesquisa é exploratória e descritiva. A abordagem descritiva tem como objetivo fornecer informações robustas sobre um tema, sem a interferência direta do pesquisador (Wazlawic, 2014). Também pode ser pode ser desenvolvida com o propósito de identificar as interações entre as variáveis (Gil, 2017).

A pesquisa exploratória é vista como a fase inicial do processo de pesquisa, pois não necessariamente o autor tem um objetivo ou hipótese definida (Wazlawic, 2014). Essa pesquisa busca proporcionar ao autor uma compreensão mais aprofundada do problema, tornando-o mais explícito e facilitando a construção de hipóteses. Esta abordagem, geralmente é flexível, pois abrange vários aspectos, como fenômeno estudado ou fatos (Gil, 2017).

Quanto aos procedimentos técnicos é uma pesquisa bibliográfica. A pesquisa bibliográfica envolve a análise de testes, artigos, e outros recursos literários (Wazlawic, 2014).

A pesquisa bibliográfica, será realizada com base em materiais previamente publicados, livros, teses, recursos *online*, entre outros (Gil, 2017).

De acordo com Gil (2017), a pesquisa bibliográfica se desenvolve a partir das seguintes etapas:

- Escolha do tema de pesquisa: Ataques cibernéticos utilizando engenharia social;
- Levantamento bibliográfico preliminar: Foram considerados os últimos cinco anos para assegurar uma pesquisa atualizada, podendo haver exceções de literatura clássica;
- Formulação do problema: nessa etapa foi formulado o problema de pesquisa: Quais são os tipos de ataques de engenharia social na computação e como se proteger?

- Busca das fontes: Na busca, utilizou-se plataformas como periódicos da CAPES, Google Scholar, entre outras. Houve uma filtragem das publicações, com a separação com base em sua relevância para a pesquisa. A categorização foi realizada com base em leitura dos resumos, classificando-os como de alta, média ou baixa relevância. Durante essa fase, o autor teve a oportunidade de fazer anotações sobre bibliografias relevantes utilizadas nos artigos consultados;
- Leitura do material: Com a posse dos materiais, é possível realizar uma filtragem seletiva, escolhendo os artigos com maior relação ao tema a ser pesquisado;
- Fichamento: Foram fichados os trabalhos de elevada relevância, uma etapa crucial que simplifica a organização de ideias para a redação do trabalho;
- Redação do texto: Por fim, o trabalho foi redigido.

4 ATAQUES CIBERNÉTICOS UTILIZANDO ENGENHARIA SOCIAL

Este capítulo identifica os ataques de engenharia social, apresentando casos reais de ataques cibernéticos e descrevendo as táticas utilizadas pelos criminosos para sua execução.

4.1 *PHISHING*

Phishing é um ataque que envolve a tentativa de enganar uma pessoa, para que ela revele informações. O termo "*phishing*" tem origem na palavra em inglês "*fishing*" (pesca), devido à semelhança entre as táticas utilizadas pelos criminosos cibernéticos e a prática de pescar." (CNN, 2023).

Os golpistas simulam pertencerem a entidade legítimas, como bancos, empresas de comércio eletrônico, serviços de pagamento ou provedores de serviços *online* para aplicarem o *phishing,* a tática neste golpe consiste em uma abordagem psicológica, como medo, urgência ou recompensa para pessoa agir rapidamente sem pensar e suspeitar do golpista (CNN, 2023).

O *phishing* visa uma abordagem para uma grande massa de usuários, tentando atingir o máximo de vítimas possíveis.

A execução do *phishing* serve como a base para a execução dos golpes, grande parte dos ataques de engenharia social utilizam alguma técnica de *phishing*.

4.1.1 *PHISHING* POR E-MAIL

O ataque de *phishing* por e-mail os golpistas utilizam a ferramenta de correio eletrônico para a execução do *phishing*, o atacante envia *e-mails* se passando por uma entidade confiável e solicitam que clique em *links* maliciosos ou forneça dados pessoais. A Figura 3 mostra uma tentativa de *Phishing* via e-mail,

Figura 3 – Ataque de *phishing* por e-mail

Fonte: De autoria própria.

O golpista tenta se passar pela empresa Registro.br. Na Figura 3 pode-se visualizar que é informado pela suposta empresa que o domínio comprado está prestes a vencer, que se o pagamento não for efetuado até a data de vencimento o domínio seria suspenso. Observa-se que o atacante utiliza a mesma formatação de e-mail da própria empresa Registro.br, sendo extremamente difícil a identificação de um golpe. Ainda no mesmo golpe, o golpista encaminha um anexo com um boleto, conforme ilustrado na Figura 4.

Figura 4 – Boleto do criminoso no ataque de *phishing*

FATURA DE REGISTRO

registro.br

05.506.560/0001-36
Núcleo de Informação e Coordenação do Ponto BR - NIC.BR
Av. das Nações Unidas, 11541, 7º andar - Brooklin Paulista
04578-000 São Paulo - SP

NÚMERO	DATA DE EMISSÃO	VENCIMENTO	CÓDIGO DE VERIFICAÇÃO
EMP06 43262549	01/11/2023	09/11/2023	KJNuK1LJlb5HXuBfSc8wpGFv4a N3AtLiM2OpXzRwUbYs2j9sQv7f

DISCRIMINAÇÃO DOS SERVIÇOS
Registro de dominio
Serviços de e-mail
Manutenção de 30/09/2023 a 31/10/2023
ref. 43262549

Tributos: COFINS 7,6%

VALOR TOTAL: R$ 983,80

23793.38029 60000.837413 18006.333308 8 95290000098380

OUTRAS INFORMAÇÕES
1. Atividade não sujeita a incidência do Imposto sobre Serviços (ISS) conforme decisão judicial proferida nos autos do processo nº 0109093-55.2008.8.26.0053, 8º Vara da Fazenda Pública do Estado de São Paulo, transitada em julgado em 12.08.2016.
2. O NIC.br declara, para fins de não incidência na fonte do IRPJ, da CSLL, da COFINS e da contribuição para PIS/PASEP, ser associação sem fins lucrativos, conforme art. 64 da Lei nº 9430/1996 e atualizações e Instrução Normativa RFB nº 1.234/2012.

Fonte: De autoria própria.

O boleto enviado possui bastante semelhança com o boleto genuíno da empresa Registro.br, tal como apresentado na Figura 5, que exibe um exemplo do boleto autêntico emitido pela empresa Registro.br.

Figura 5 – Boleto genuíno da empresa Registro.br

FATURA DE REGISTRO

nic.br

05.506.560/0001-36
Núcleo de Informação e Coordenação do Ponto BR - NIC.br
Av. das Nações Unidas, 11541, 7º andar - Brooklin Paulista
04578-000 - São Paulo - SP

NÚMERO	DATA E HORA DE EMISSÃO	CÓDIGO DE VERIFICAÇÃO
REG03 37240310	02/12/2021 12:03:20	GY2mowQCAdDyi67Asw4BJF wwEwKQSoTLzkjomDH59UGv

TOMADOR DE SERVIÇOS

Nome Empresarial: Cooperat de Crédito Rural do Vale do Araguaia Ltda
CNPJ: 024.830.879/0001-67
Endereço: Terceira Avenida, 6-A, Centro
75830-000, Mineiros, GO, BR

PAGA

DISCRIMINAÇÃO DOS SERVIÇOS

Registro de domínio - sicoobmineiros.com.br
Manutenção de 08/12/2021 a 07/12/2023
ref. 36144840

Tributos: COFINS 7,6%

VALOR TOTAL: R$ 76,00

OUTRAS INFORMAÇÕES

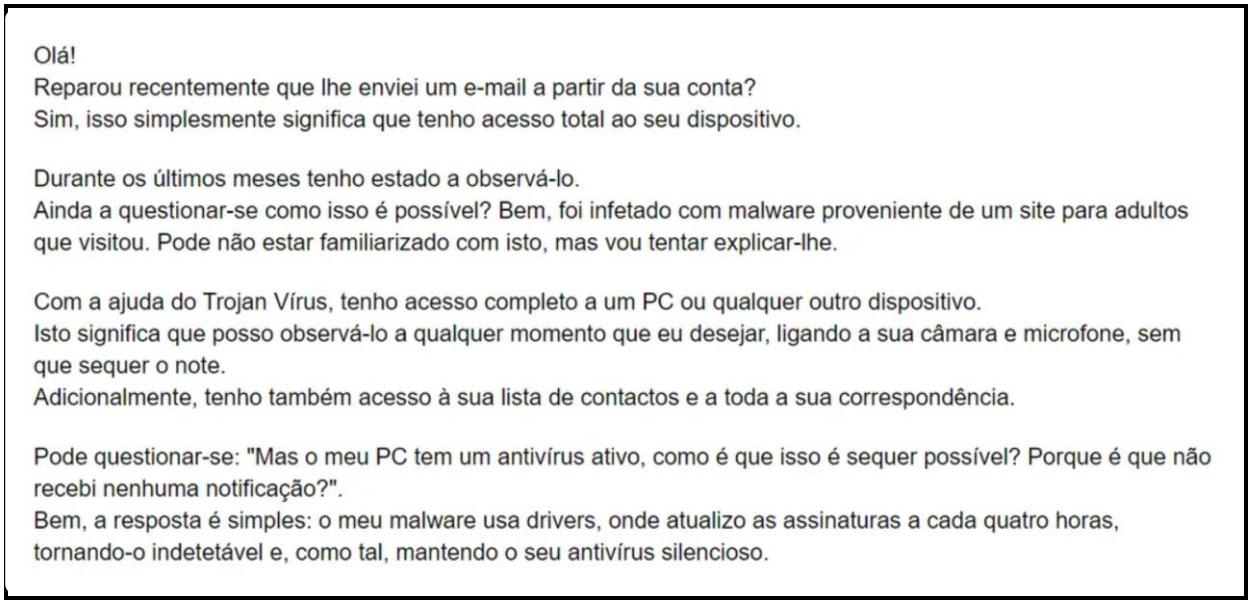
1. Atividade não sujeita a incidência do Imposto sobre Serviços (ISS) conforme decisão judicial proferida nos autos do processo nº 0109093-55.2008.8.26.0053, 8ª Vara da Fazenda Pública do Estado de São Paulo, transitada em julgado em 12.08.2016. Emissão de nota fiscal vedada pela Municipalidade de São Paulo. Fatura emitida com fundamento no artigo 1º da Lei nº 8.846/94 e Solução de Consulta (COSIT) nº 295/14.
2. O NIC.br declara, para fins de não incidência na fonte do IRPJ, da CSLL, da COFINS e da contribuição para PIS/PASEP, ser associação sem fins lucrativos, conforme art. 64 da Lei nº 9.430/1996 e atualizações e Instrução Normativa RFB nº 1.234/2012.
3. Quitado em 07/12/2021 via boleto número 36144840

Fonte: De autoria própria.

Os criminosos virtuais sempre buscam formas de serem ardiloso em seus ataques, outra forma de provar autenticidade neste ataque é utilizar como remetente do e-mail, o próprio e-mail da vítima. Ao enviar um e-mail, os sistemas de correio eletrônico não verificam o remetente, portanto o hacker utiliza esta falha para realizar o ataque.

Nota-se que a Figura 6 mostra outra tentativa de um ataque de *phishing* via e-mail.

Figura 6 – E-mail enviado do golpista em um ataque de *phishing*



Olá!
Reparou recentemente que lhe enviei um e-mail a partir da sua conta?
Sim, isso simplesmente significa que tenho acesso total ao seu dispositivo.

Durante os últimos meses tenho estado a observá-lo.
Ainda a questionar-se como isso é possível? Bem, foi infetado com malware proveniente de um site para adultos que visitou. Pode não estar familiarizado com isto, mas vou tentar explicar-lhe.

Com a ajuda do Trojan Vírus, tenho acesso completo a um PC ou qualquer outro dispositivo.
Isto significa que posso observá-lo a qualquer momento que eu desejar, ligando a sua câmara e microfone, sem que sequer o note.
Adicionalmente, tenho também acesso à sua lista de contactos e a toda a sua correspondência.

Pode questionar-se: "Mas o meu PC tem um antivírus ativo, como é que isso é sequer possível? Porque é que não recebi nenhuma notificação?".
Bem, a resposta é simples: o meu malware usa drivers, onde atualizo as assinaturas a cada quatro horas, tornando-o indetetável e, como tal, mantendo o seu antivírus silencioso.

Fonte: Rohr, 2020.

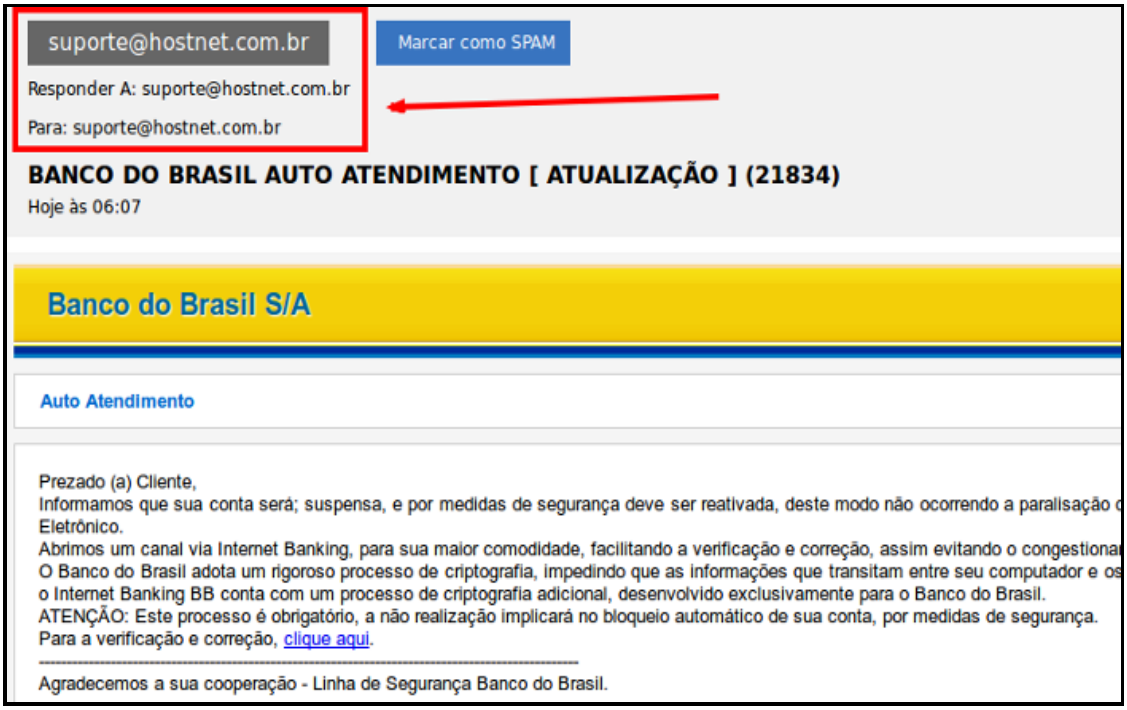
Neste ataque o golpista utiliza da fragilidade do sistema de e-mail, para persuadir a vítima. O criminoso afirma que o dispositivo da vítima foi infectado por *malware* e que ele tem acesso a todas as informações armazenadas no dispositivo.

A técnica utilizada pelo golpista se chama *spoofing*, esta técnica consiste na falsificação do cabeçalho de e-mail, permitindo a utilizada nos ataques para falsificar o endereço de remetente, para que pareça que o e-mail enviado seja genuíno.

No ataque da Figura 6, o atacante utiliza a técnica de *spoofing* para induzir a vítima que o seu dispositivo foi infectado e que ele tem o acesso total a sua máquina.

Na Figura 7 pode-se visualizar como ficaria o cabeçalho de um ataque utilizando o *spoofing*.

Figura 7 – Cabeçalho de um ataque utilizando técnica de s*poofing*



Fonte: Hostnet, 2024.

4.1.2 *PHISHING* POR SMS OU *SMISHING*

O *smishing* é uma forma de ataque de *phishing* que utiliza como ferramenta para comunicação mensagens de texto enviadas para dispositivos móveis, os golpistas utilizam o sistema de SMS das operadoras para encaminhar mensagens às suas vítimas.

O ataque de *smishing* tem como objetivo o roubo de informações e acessos a sistemas e a propagação de *malware* e *ransomware* no dispositivo.

A Figura 8 apresenta uma tentativa de *smishing*, no qual o golpista tenta se passar por um banco, solicitando à vítima que entre no *link* para resgatar prêmios no sistema de pontos do banco.

Figura 8 – Ataque *smishing*

Fonte: De autoria própria.

Ao entrar no *link* a vítima é redirecionada a um site falso que solicita as informações bancárias, conforme mostrado na Figura 9.

Figura 9 – Página de autenticação falsa do Banco do Brasil

Fonte: QuatroCantos, 2015.

No exemplo da Figura 8, o atacante tenta coletar as informações bancárias da vítima. Com esses dados, o golpista pode acessar a conta bancária e realizar transações financeiras não autorizadas.

Uma vez que o atacante possua as informações, o golpista pode transferir dinheiro, fazer compras ou realizar outras atividades fraudulentas, causando a vítima prejuízos financeiros.

4.1.3 *PHISHING* POR REDES SOCIAIS OU *PHARMING*

O *pharming* é uma técnica de engenharia social que utiliza como ferramenta de comunicação as redes sociais tais como, Instagram, Facebook, Whatsapp, entre outras. Os golpistas utilizam destas plataformas de rede sociais para entrar em contato com a vítima e aplicar o *phishing*.

Na pesquisa realizada pela empresa Kaspersky foi comprovado que o Brasil é o país que mais sofre de golpes de p*harming* via Whatsapp no mundo (Ferreira, 2023).

O ataque não requer um conhecimento técnico avançado fazendo com que os golpistas o utilizem com mais frequência.

Neste ataque os golpistas utilizam de duas formas para obter um perfil na rede social: na primeira, eles criam um perfil que seja muito semelhante ao original, copiando as fotos, publicações e o próprio nome do perfil e finge ser uma empresa genuína. O segundo método, os golpistas tentam roubar um perfil genuíno, utilizando de outras técnicas da engenharia social.

Este primeiro exemplo é mostrado na Figura 10, a criação de um perfil da empresa Lojas Americanas falso na rede social Instagram, no qual o mesmo divulga produtos com preços inferiores ao mercado

Figura 10 – Anúncio falso das Lojas Americanas

Fonte: Oliveira, 2019.

Na Figura 11 é mostrado o verdadeiro preço do mesmo equipamento na verdadeira Lojas Americanas.

Figura 11 – Anúncio verdadeiro das Lojas Americanas

Fonte: Americanas, 2023.

Conforme apresentado na Figura 10, o golpista realiza a criação de um perfil da empresa Lojas Americanas, utilizando um nome extremamente parecido com o perfil, foto do perfil e publicações. Pode-se notar a extrema semelhança entre os dois perfis, e com esta semelhança o golpista utiliza desta suposta imagem para enganar suas vítimas e aplicar o *phishing*.

Outra forma que os golpistas realizam o *phishing* é através de uma rede social verdadeira. O criminoso toma o controle do perfil através de manipulações de *phishing*. O atacante utiliza alguma técnica de *phishing* para entrar em contato com a vítima, solicitando dados de acesso tais como: senha, usuário, código de segurança, entre outros.

Após o golpista ter acesso a conta pessoal da vítima, começa a utilizá-la para aplicar golpes na rede de amigos da vítima. Com o acesso de uma conta verdadeira, o criminoso transmite mais confiança no seu ataque, pois as vítimas conhecem o perfil e julgam ser verdadeiras as ofertas do atacante.

Por exemplo, ocorreu um caso com o professor Carlos Rodrigues, de 57 anos, quando um hacker invadiu a sua conta e começou a anunciar vários produtos em suas redes sociais, com valores extremamente atrativos (Rohr, 2020). conforme apresentado na Figura 12.

Figura 12 – Perfil da vítima do ataque de *Pharming*

Fonte: Rohr, 2020.

Em 2023, um golpe que ganhou destaque no Brasil foi o “urubu do PIX”. Neste ataque os golpistas invadem as redes sociais de uma pessoa legítima e oferecem uma oferta de investimento que prometem retornos extraordinários em um curto período.

Na Figura 13, pode-se visualizar a oferta publicada pelos atacantes.

Figura 13 – Ataque *Pharming* “urubu do PIX”

Fonte: Blasi, 2023.

Após atrair a atenção da vítima, o golpista busca transmitir uma sensação de segurança, afirmando que o investimento é genuíno e legitimo. Para reforçar a ideia, os atacantes afirmam ser o proprietário do perfil da rede social que foi comprometida. E alegam ter realizado o investimento e se beneficiaram, trazendo ainda mais legitimidade ao golpe.

O golpe torna-se ainda mais eficiente quando a conta invadida é de uma figura pública de influência. Isso ocorre devido ao alcance de suas publicações e sua legitimidade por se tratar de influenciador digital, sendo improvável que um influenciador digital se envolva em esquemas fraudulentos.

4.1.4 *PHISHING* POR LIGAÇÃO TELEFÔNICA OU *VISHING*

O *phishing* por Ligação telefônica ou *vishing* é uma técnica de *phishing* que utiliza como ferramenta as ligações telefônicas como meio de comunicação com suas vítimas.

Esta abordagem é utilizada pelos atacantes para conseguir acessos a redes sociais e contas bancárias. O golpista aborda a vítima fingindo ser de uma empresa de legitima e solicita à vítima que informe o código de segurança enviado no SMS, após a vítima informar o código de segurança, o golpista tem acesso total a rede social e pode realizar alterações no cadastro com o intuito que alvo perca o acesso da rede social.

Golpistas também pode utilizar a técnica para convencer o alvo a enviar dinheiro. O golpista entra em contato com a vítima informado que faz parte de uma instituição financeira, solicitando a vítima que envie dinheiro, com o pretexto de falhas no sistema, entre outros.

Um caso noticiado pelo G1 (2021), a vítima José de Paula, havia anunciado a venda de um carro, os golpistas fingiram ser um funcionário do site, na ligação dizendo,

Golpista: Tem uma atualização aqui na nossa plataforma que se encontra pendente no seu anúncio. Estarei fazendo ela agora para o senhor, ok?

José: Ok.

Golpista: Verifique a sua caixa de mensagem.

José: Eu vou dar uma olhada aqui.

Golpista: Verifique e nos informe, aguardo em linha.

José: Falou!”

José: Aqui, deixa eu falar com você. Isso aí está parecendo já é trote, porque meu WhatsApp já saiu do meu telefone.

Golpista: Pode ficar despreocupado. Segurança total.

Neste caso os estelionatários conseguiram realizar uma transferência bancária. Jose relatou, “Infelizmente, dois que caíram, um amigo meu e um primo. O meu amigo realizou um depósito de R$ 720, mas outro depósito de R$ 100. E meu primo foi só um depósito de R$ 400”, contou José de Paula.” (G1, 2021).

Ao analisar o golpe, os atacantes utilizaram técnicas de *phishing* utilizando método *vishing* para obter a rede social Whatsapp da vítima e logo após aplicou método de *pharming* nos contatos da vítima.

Outro ataque que utiliza a técnica de *vishing* são os golpes voltados a instituição financeiras. Golpistas estão burlando o identificador de chamadas telefônicas para se passar por bancos e aplicar fraudes (G1, 2024).

Uma consultora de vendas, de Santa Cruz do Sul, no Rio Grande do Sul, que prefere não se identificar, pensou que a ligação era do banco. O número que apareceu no celular era o do *Call Cente*r, que ela tinha na própria agenda do telefone (G1, 2024).

O golpista perguntou se ela tinha feito compras e pagamentos de boletos no valor de R$ 16 mil. Para cancelar as despesas e receber o dinheiro de volta, ela teria que transferir para outra conta corrente o mesmo valor. E foi o que a vítima fez (G1, 2024).

A vítima relatou, “Eu não só perdi uma parte de uma poupança, como também foram compras no cartão de crédito, eu precisei pagar o cartão de crédito para não virar uma bola de neve. Tive que fazer um empréstimo para poder pagar” (G1, 2024).

4.1.5 *PHISHING WHALING*

Whaling é a forma específica de ataque de *phishing* que direciona os ataques para alvos influentes, como celebridades, executivos de empresas, líderes, figuras de destaque, entre outros.

De acordo com Bertolli (2021), os cibercriminosos analisam as mídias sociais e informações públicas da empresa para estabelecer um perfil e um plano de ataque.

Podem também usar *malware* e *rootkits* para se infiltrar na rede: um e-mail proveniente da conta do CEO é muito mais eficaz que uma conta de e-mail falsificada.

Em 2016, o principal diretor financeiro da empresa Mttel foi alvo de um ataque de *whaling* através de um e-mail fraudulento. O golpista se passou pelo recém-nomeado CEO, apresentando uma solicitação de transferência recorrente para um fornecedor na China. Este golpe gerou uma perda de 3 milhões de dólares para a empresa Mttel (Nadeem, 2023).

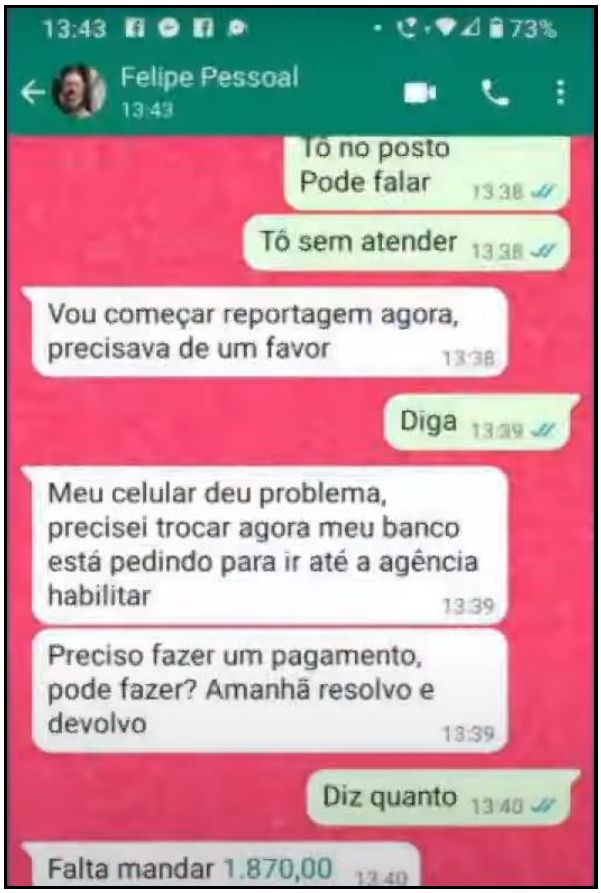
4.1.6 *PHISHING* UTILIZANDO FERRAMENTA DE INTELIGÊNCIA ARTIFICIAL

Com o avanço constante da tecnologia de inteligência artificial, os golpistas estão utilizam da tecnologia conjunta das táticas de *phishing* para aplicar golpes em suas vítimas, passando mais legitimidade ao aplicar os golpes.

A capacidade de utilizar IA facilita os ataques de *phishing,* fazendo com que os criminosos podem utilizar uma variedade de ferramentas sofisticadas, permitindo-lhes a replicação com precisão da voz, imagens e fotografias de indivíduo.

De acordo com TV Cultura (2024), O jornalista Felipe Laud passou por uma tentativa de *pharming*, o golpista utilizou uma conta de Whatsapp falso, com a foto de perfil genuína do jornalista, o atacante entrou em contato com a mãe da vítima fingindo se passar pelo jornalista, dizendo que precisa de dinheiro, conforme demostrado na Figura 14.

Figura 14 – Conversa do golpista com mãe da vítima



Fonte: TV Cultura, 2024.

Ao analisar a Figura 14, observa-se que o atacante utiliza de método do ataque de *pharming* para passar confiança e legitimidade para mãe de Felipe, com a ajuda da IA, o golpista cria um áudio com a voz de Felipe, dizendo, “É porque não vou conseguir ir ao banco hoje, mãe. Não vai dar tempo, mas amanhã cedo já resolvo e te mando.”, de acordo com Felipe a voz era idêntica a dele (TV Cultura, 2024).

Os atacantes também utilizando as ferramentas de IA para ataques de *phishing* por e-mail, utilizando IA para personalizar e segmentar e-mails de *phishing*, assim tornando o ataque mais convincentes e difíceis de detectar.

“A inteligência artificial ainda é capaz de analisar e monitorar o tráfego de e-mail, aprender os padrões normais de comunicação e criar mensagens autênticas, assim aumentando a taxa de sucesso nos golpes” (Check Point, 2024).

De acordo com Chen e Magromo (2024), um funcionário financeiro de uma empresa multinacional pagou US$ 25 milhões a fraudadores que usaram tecnologia *deepfake* cridas por IA para se passar por diretor financeiro da empresa em uma videoconferência.

“O golpe fez com que o trabalhador fosse levado a participar de uma videochamada com o que ele pensava que fossem vários outros membros da equipe, mas todos na verdade eram criações falsas” (Chen e Magramo, 2024).

“Chan disse que o trabalhador ficou desconfiado depois de receber uma mensagem supostamente do diretor financeiro da empresa com sede no Reino Unido. Inicialmente, o trabalhador suspeitou que se tratasse de um e-mail de *phishing*, pois falava da necessidade da realização de uma transação secreta” (Chen e Magramo, 2024).

“No entanto, o trabalhador deixou de lado as suas primeiras dúvidas após a vídeo chamada porque outras pessoas presentes pareciam e soavam como colegas que ele reconhecia, disse Chan” (Chen e Magramo, 2024).

O golpe foi utilizado o *phishing* por e-mail para atraia a atenção do colaborador e após utilizado a reunião com os supostos dirigentes criados por IA para dar legitimidade ao ataque.

Com a utilizando de IA nos golpes demostrado, vemos que criação fraudes e ataques ficam cada vez mais sofisticadas.

4.2 *BAITING*

Baiting é um ataque que utiliza código malicioso para infectar o dispositivo e coletar dados, o criminoso atrai a vítima com ofertas em anúncios, jogos, música ou *software* gratuitos, após a vítima executar o código, o criminoso terá acesso aos dados armazenados no dispositivo da vítima.

Este código malicioso pode ser executado através de arquivos baixados pela Internet, dispositivos de armazenamento, como *Pendrive* e *DVD*, entre outros.

Um dos ataques se chama *Rubber Ducky* ou *BadUSB*, “O aparelho quando é conectado a um dispositivo eletrônico simula o funcionamento de um teclado e executa uma sequência de ações no dispositivo, a fim de executar um programa ou fazer várias outras tarefas de forma automática.” (Wikipidia, 2022).

Uma empresa recebeu um envelope com um falso cartão de presente da empresa BestBuy e um *pen drive USB*. no cartão havia a orientação de ligar o pen drive em um computador para acessar os produtos do cartão presente. após análises dos especialistas de segurança da empresa verificaram previamente o possível ataque. (Rezende, 2022).

O b*aiting* é mais comum aos usuários que utilizam matérias proveniente da pirataria.

A pirataria é uma prática que prejudica diretamente a sua segurança digital e o da empresa. Esse tipo de arquivo facilita o acesso de invasores ao seu computador e celular, facilitando a exposição e o vazamento dos seus dados (Oliveira, 2019).

Estudos mostram que mais da metade das pessoas baixam arquivos ilegais em nosso continente, e o número não para de crescer. Existem diversos sites que facilitam esse processo, os mais famosos incluem Pirate Bay e o Mega, já antigos na internet (Oliveira, 2019).

Em 2019 a loja Renner sofreu um ataque de *ransomware*, este ataque resultou na indisponibilidade dos sistemas e operações (Exame, 2019).

De acordo com a varejista, os ataques solicitaram 20 milhões de dólares em criptomoedas para recuperação dos dados, a varejista negou as negociações que resultou no sistema inoperante (Exame, 2019). Não foi informado pela empresa como os atacantes realizaram a invasão.

Ao baixa um *software* pirata qualquer dispositivo está sujeito a um ataque de *ransomware*, podendo resultar em perdas irreparáveis.

4.3 *TAILGATING*

“Através de táticas de engenharia social, um *hacker* ganha proximidade com alguém com o objetivo de invadir um dispositivo, rede, área restrita ou qualquer coisa que seja interessante para o roubo de dados, informações e dinheiro.” (Klusaitė, 2023).

O *tailgating* é uma técnica utilizada para obter acesso não autorizado a uma instalação física ou informações confidenciais. Nesse contexto, "*tailgating*" envolve uma pessoa não autorizada seguindo de perto um funcionário autorizado através de uma entrada segura, como uma porta com controle de acesso, sem apresentar sua própria credencial de acesso.

Tailgating pode resultar em roubo de dispositivos, onde invasores roubam computadores e outros dispositivos para vendê-los ou realizar ataques posteriores. Também pode levar ao roubo de dados, quando funcionários deixam documentos confidenciais acessíveis, permitindo que invasores com acesso físico obtenham informações sensíveis (Check Point, 2024).

Além disso, o acesso físico a dispositivos comprometidos por meio de *tailgating* pode contornar defesas cibernéticas e permitir a instalação de *malware* como *ransomware* ou *keyloggers*. Podendo levar a organização a desativação temporária ou permanentemente, mantendo-a refém (Check Point, 2024).

Um dos pretextos frequentemente usados é afirmar ter perdido ou esquecido a identificação de funcionário, solicitando a entrada junto com um colega legítimo. Outro disfarce comum é se passar por um motorista de entregas, aproveitando a confiança associada a essa função. Além disso, os invasores podem deliberadamente aparentar estar com as mãos ocupadas ao se aproximarem de uma porta, aumentando a probabilidade de que alguém segure a porta para eles (Check Point, 2024).

A falta de vigilância também é explorada, com invasores se aproveitando de portas deixadas abertas por funcionários distraídos. Por fim, se um invasor conseguir roubar a identificação ou dispositivo de um usuário autorizado, ele pode copiar as credenciais para se passar por um funcionário legítimo e obter acesso indevido. Essas

estratégias destacam a importância de uma conscientização rigorosa sobre segurança entre os funcionários e a implementação de medidas de controle de acesso adequadas para prevenir esses tipos de ataques (Check Point, 2024).

O caso mais conhecido de *tailgating* é o de Frank William Abagnale Jr., conhecido como “Mestre da Fraude”. Frank era um especialista em engenharia social e utilizava das suas habilidades para persuadir suas vítimas. Um dos golpes mais famosos de Frank foi quando se passou por um piloto da companhia aérea PanAm. Utilizando um uniforme falso, crachá de identificação e até mesmo um certificado de piloto falsificado, Frank conseguia viajar pelo mundo de forma gratuita, apresentando-se como um verdadeiro piloto da PanAM. Esta estratégia permitiu ao Frank acesso privilegiado e viagens sem custo (Canal Ciências Criminais, 2023).

4.4 *SCAREWARE*

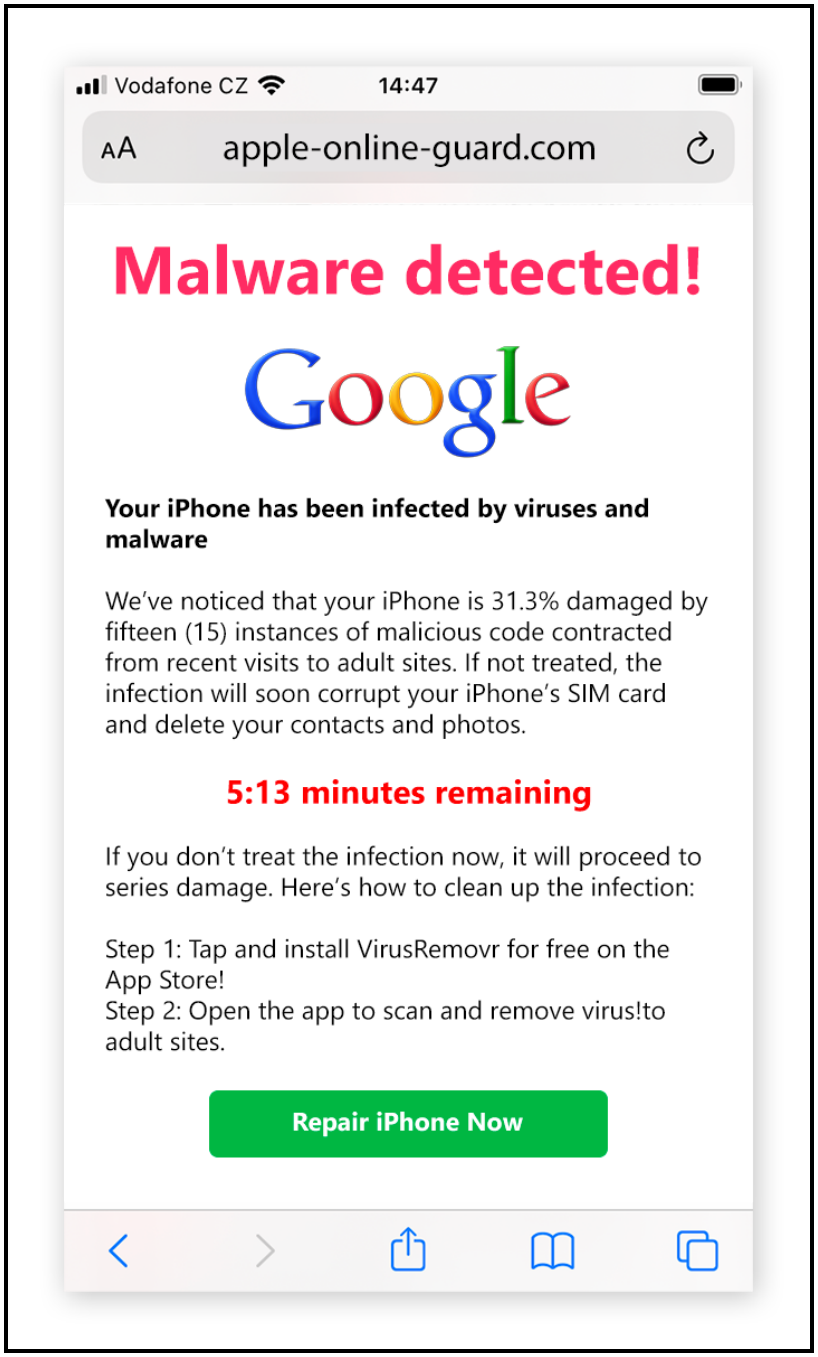
O *scareware* conhecido como “falso *software* de segurança” ou “falso antivírus”, é um tipo de ataque que é projetado para assustar e enganar a vítima, fazendo com que ela acredite que seu dispositivo pode estar infectado por vírus, *malware* ou ameaças graves de segurança. O golpe é muito realizado via propagandas e *pop-up* maliciosos. A Figura 15 apresenta um ataque de *scarewares*, no qual os atacantes criam um *pop-ups* de vírus falsos, onde é informado, que o computador da vítima está com 5 vírus.

Figura 15 - Ataque *scarewares* pop-up

Fonte: Freda, 2021.

Diversas abordagens de *scareware* buscam imitar fontes confiáveis, tais como o Google e podem empregar uma contagem regressiva para criar uma sensação de urgência e medo (Freda, 2021), conforme mostrado na Figura 16.

Figura 16 - Ataque *scarewares* pelo navegador



Fonte: Freda, 2021

“Esses *pop-ups* de vírus de computador podem até ser ataques de *spoofing*, fazendo parecer que vêm diretamente do seu sistema operacional ou de outra fonte confiável.” (Buxton, 2021).

Os atacantes frequentemente empregam botões falsos, como "Fechar", em anúncios que, ao serem clicados, instalam *malware* nos dispositivos das vítimas. Esse *malware* pode se assemelhar a um *software* antivírus legítimo, porém, sua eficácia é nula na proteção contra ameaças reais. Além disso, pode facilitar a entrada de outros *malwares*, comprometendo a segurança do dispositivo (Buxton, 2021).

Após o usuário aceitar a reparação deste suposto *malware* detectado no dispositivo, o golpista pode encaminhar a vítima para a compra de um *software* falso ou *software* sem utilidade, com a promessa de que resolverá o problema de segurança. No ato da compra a vítima informa dados possais, cartão de crédito, entre outros, podendo utilizar os dados em atividades fraudulentas (Buxton, 2021).

Além disso, o usuário pode ser redirecionado para sites que tentam extrair mais informações pessoais ou infectar o dispositivo com *malware*.

O objetivo do *scareware* é criar pânico ao usuário e assim fazendo com que o usuário tome de decisões precipitadas, o golpista tem como objetivo lucrar com a venda de produtos ou serviços falsos ou, até mesmo, obter acesso indevido ao sistema da vítima.

4.5 *WATERING HOLE*

*"*Um ataque *watering hole* é uma exploração de segurança na qual o invasor busca comprometer um grupo específico de usuários finais, infectando sites que os membros do grupo costumam visitar.” (Minuto da segurança, 2021).

O objetivo dos atacantes é explorar a confiança dos usuários nos sites que visitam regularmente, aproveitando-se de sua familiaridade com esses locais para infectar seus dispositivos ou roubar informações confidenciais (Minuto da segurança, 2021).

Inicialmente, o invasor identifica um site ou serviço frequentemente utilizado pela vítima pretendida, caracterizado por baixos níveis de segurança e alta popularidade entre o público-alvo (Minuto da segurança, 2021).

Após selecionar o site alvo, o invasor compromete sua segurança, inserindo um código malicioso, geralmente em JavaScript ou HTML. Quando a vítima visita o site comprometido, o código malicioso é acionado, desencadeando uma série de explorações para infectar o computador da vítima (Minuto da segurança, 2021).

O *download* do *malware* pode ser realizado automaticamente ou mediante um falso aviso, instruindo o usuário para realizar *download* do código malicioso. (Minuto da segurança, 2021).

Após a ativação da carga no computador da vítima, o invasor pode acessar outros recursos na rede e usar esse dispositivo para lançar ataques subsequentes, como pivôs para alcançar outros objetivos. Estes podem incluir a coleta de informações sobre a vítima, o uso do computador infectado como parte de uma rede de *bots* ou tentativas de explorar outros sistemas dentro da rede da vítima (Minuto da segurança, 2021).

Em julho de 2017, ocorreu um ataque de *malware NotPetya*, um grupo de hackers russo. O ataque foi realizado utilizando a técnica do *watering hole*, no qual os hackers identificaram e comprometeram um site frequentemente visitado pelos usuários alvo. Neste caso, o site governamental serviu como ponto de entrada para os invasores (Compugraf, 2020).

Quando os usuários acessaram o portal comprometido, inadvertidamente baixaram o *malware*, sem perceberem. Como resultado, os HD dos computadores das vítimas foram apagados, causando danos significativos e interrupções nas operações (Compugraf, 2020).

Este incidente destaca a eficácia do ataque de *watering hole* como um meio de distribuição de *malware*, aproveitando-se da confiança dos usuários em sites conhecidos para disseminar ameaças cibernéticas.

4.6 *QUID PRO QUO*

Quid pro quo significa “algo por algo”, na engenharia social é uma tática utilizada pelos engenheiros para fazer uma “troca de favores”.

O ataque de *quid pro quo* acontece quando um *hacker* solicita informações confidenciais de alguém em troca de algo (ClearSale, 2022).

Podem ser tratados dois cenários para este ataque: o primeiro consiste que a proposta encaminhada para a vítima foi genuína e aceitável, ou seja, a vítima não tinha ciência de que poderia ser enganada.

O segundo cenário envolve a ética ou legalidade da proposta, na qual a pessoa que recebeu a proposta pode estar sendo subordinada, assediada ou outros comportamentos antiéticos.

> Digamos que você seja contatado por um funcionário de TI que ofertas para realizar uma auditoria em seu computador para remover possíveis vírus que possam diminuir o desempenho de seu computador. Mas para isso, ele precisa do seu login e senha. Nada poderia ser mais natural! Você fornece a ele essas informações sem qualquer discussão: afinal, você vem reclamando da lentidão do seu computador há meses. Exceto que esta troca de boa vontade pode não ser boa, e que você pode ter acabado de cair na armadilha de um ataque *quid pro quo*. Os ataques quid pro quo são baseados em manipulação e abuso de confiança. Assim, eles se enquadram na categoria de técnicas de engenharia social, tal como ataques de *phishing* (incluindo *spear phishing* e ataques baleeiros ou *whaling attacks*), *baiting* ou pretexto (Nadeem, 2022).

A técnica pode apresentar sérios danos que afetam a segurança e integridade de um sistema e dados. No ataque pode houver manipulação e divulgação de dados pessoais, violando seriamente a privacidade de terceiro, além de poder criar diversas vulnerabilidades de segurança, dando ao atacante pode de obter acessos não autorizada aos em sistema e informações confidenciais.

4.7 *OPEN SOURCE INTELLIGENCE*

OPEN SOURCE INTELLIGENCE ou Inteligência de Fonte (OSINT) Aberta é uma técnica utilizada pelos atacantes que visa isolar a vítima coletando e analisando informações públicas. Os golpistas utilizam ferramentas como redes sociais, fóruns *online*, mídia, documentos públicos, fontes de informações governamentais públicas, entre outras, para coletar informações sobre a vítima.

Em fevereiro de 2013, o hacker Marcel-Lehel Lazăr, conhecido como Guccifer, realizou uma invasão aos e-mails de políticos americanos, tais como de George W. Bush, ex-presidente dos Estados Unidos, Tony Blair ex-primeiro-ministro do Reino Unido e Hillary Clinton ex-secretária de Estado dos Estados Unidos, entre outros (Iamarino, 2021).

Guccifer era um ex-taxista que não possuía conhecimento avançado de *hacking*, o método para invasão as contas foi a procura de informações públicas de suas vítimas. O invasor procurava dados públicos como, nome de parentes, data de nascimento, nome dos animais de estimação, endereços, gostos pessoais, cidade de nascimento, entre outros (Iamarino, 2021).

O ataque pode gerar diversas consequências, como, violação da privacidade, caso o atacante tiver sucesso no ataque, podendo invadir os dados das vítimas e até perpetrar roubo de identidade, fraudes financeiras, entre outros.

4.8 *DUMPSTER DIVING*

A técnica *dumpster diving* ou Mergulho na lixeira, visa buscar informações, itens ou matérias que a vítima descarta no lixo.

Os golpistas analisam os padrões de descarte realizados pela vítima, após realiza uma procura nos resíduos equipamentos eletrônicos ou documentos, tais como, computadores, celulares, documentos corporativos ou pessoais, dispositivos de armazenamento, entre outros.

Após a coleta dos dados, os atacantes podem realizar uma séria de ataques, que podem ter a intenção de causar desde fraudes financeiras até roubo de identidade e ataques de engenharia social mais sofisticados.

Esta técnica pode parecer inábil, mas é um perigo eminente para quem não realiza o descarte correto dos equipamentos eletrônicos, dos documentos físicos, relatórios, entre outros. Pode-se também ser um perigo a pessoas físicas, informando dados pessoais como CPF, RG entre outros. Assim, o golpista pode ter acesso a várias informações da vítima.

Em 2014 a empresa Midwest Women's Healthcare Specialists foi condenada a pagar uma multa de 400 mil dólares pelo descarte de registro de clientes inadequados (Morris, 2014).

A empresa realizou o descarte de 1532 registros sensíveis de clientes, que foram descartados em uma lixeira durante um projeto de construção (Morris, 2014).

Como resultado, um acordo foi feito, os clientes recebendo dois anos de monitoramento de crédito, compromissos de melhoria na segurança da informação por parte da empresa e o pagamento para os clientes afetados, com

aproximadamente 1.430 clientes cujo registros foram descartados dividindo 141 mil dólares e cerca de 102 clientes cujo registros nunca foram recuperados dividindo 114 mil dólares (Morris, 2014).

Este incidente abri a possibilidade de diversos ataques de engenharia social, não apenas em termos de potencial uso indevido de informações sensíveis, mas também em custos legais e compensatórios associados à violação da privacidade dos clientes.

5 METODOS DE PREVENÇÃO AOS ATAQUES DE ENGENHARIA SOCIAL

Conforme demonstrado anteriormente, existem diversos ataques utilizando engenharia social e é de extrema importância se precaver dos ataques, visto que qualquer pessoa pode ser um alvo para os criminosos.

A base de todos os métodos de prevenção aos ataques de engenharia social é a necessidade de permanecer sempre atento e desconfiado de qualquer interação suspeita ou fora do padrão. Sendo uma prática fundamental para se precaver de possíveis ataques e reforçar a segurança pessoal e digital.

Este capítulo visa apresentar métodos de prevenção contra ataques de engenharia social.

5.1 METODOS GERAIS PARA PREVENÇÃO CONTRA OS ATAQUES

Estes métodos de prevenção podem ser aplicados a diversos tipos de ataques.

São abordadas técnicas fundamentais que fortalecem a segurança e a conscientização dos usuários, preparando-os para identificar e evitar tentativas de ataque de engenharia social.

A aplicação desses métodos é essencial para criar uma defesa contra os ataques de engenharia social.

5.1.1 PROTEÇÃO EM SITES

Uma estratégia fundamental na prevenção de ataques cibernéticos é a verificação da autenticidade dos sites.

Analisar o domínio do site é primordial para a proteção, “O domínio é basicamente, é o endereço que você digita na barra do navegador para entrar em um site. É como se fosse o endereço de sua casa digital, e, por este motivo, precisa ser único.” (Souza, 2022).

Analisar o domínio de um site é crucial para garantir a segurança na navegação, verificar a autenticidade do site para proteger os dados pessoais.

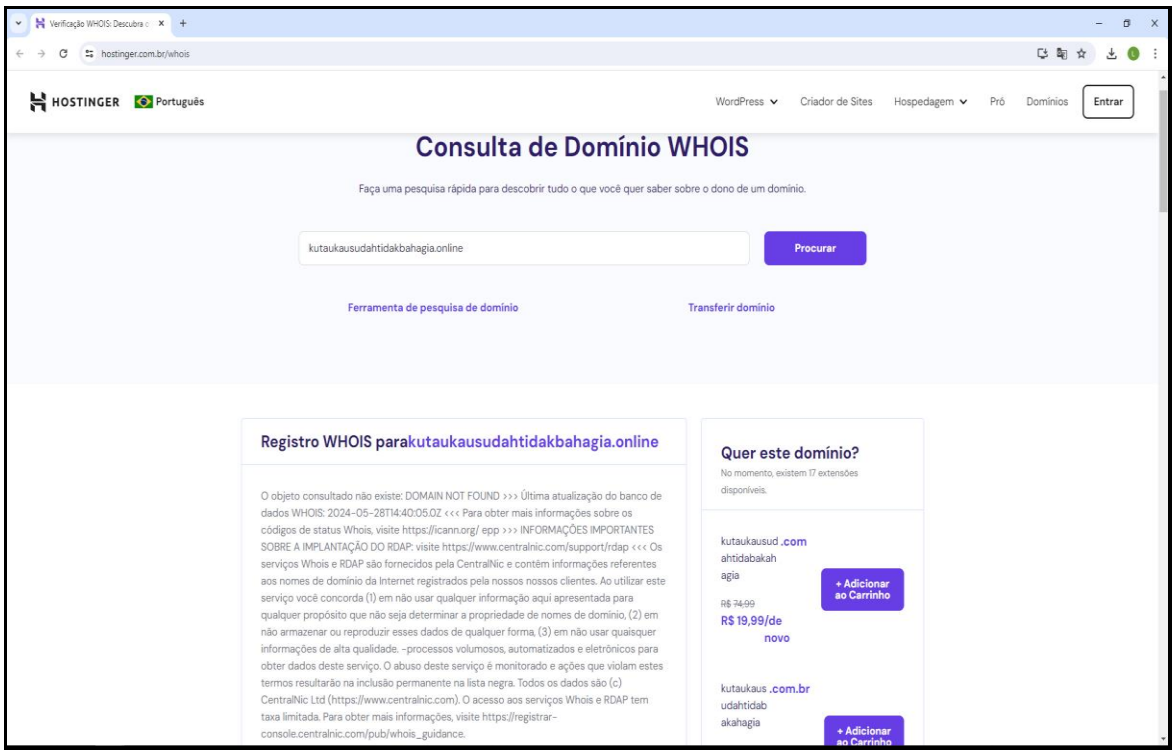
Pode-se realizar a análise e confirmar a autenticidade do domínio do site utilizando a ferramenta WHOIS. WHOIS é um serviço de banco de dados público que

permite consultar informações sobre o domínio e fornece detalhes sobre o proprietário do domínio, tais como, nome, contato, endereço e endereço do proprietário, dados técnicos e outras informações relacionadas ao registro do domínio.

Várias empresas fornecem esta ferramenta para consulta de forma gratuita, nas verificações a seguir utilizaremos a ferramenta de WHOIS pelo site hostinger.com.br.

Ao utilizar a ferramenta para verificar o domínio kutaukausudahtidakbahagia.online, pode-se verificar que este domínio atualmente encontra-se desativado e sem um proprietário, conforme ilustrado na Figura 17.

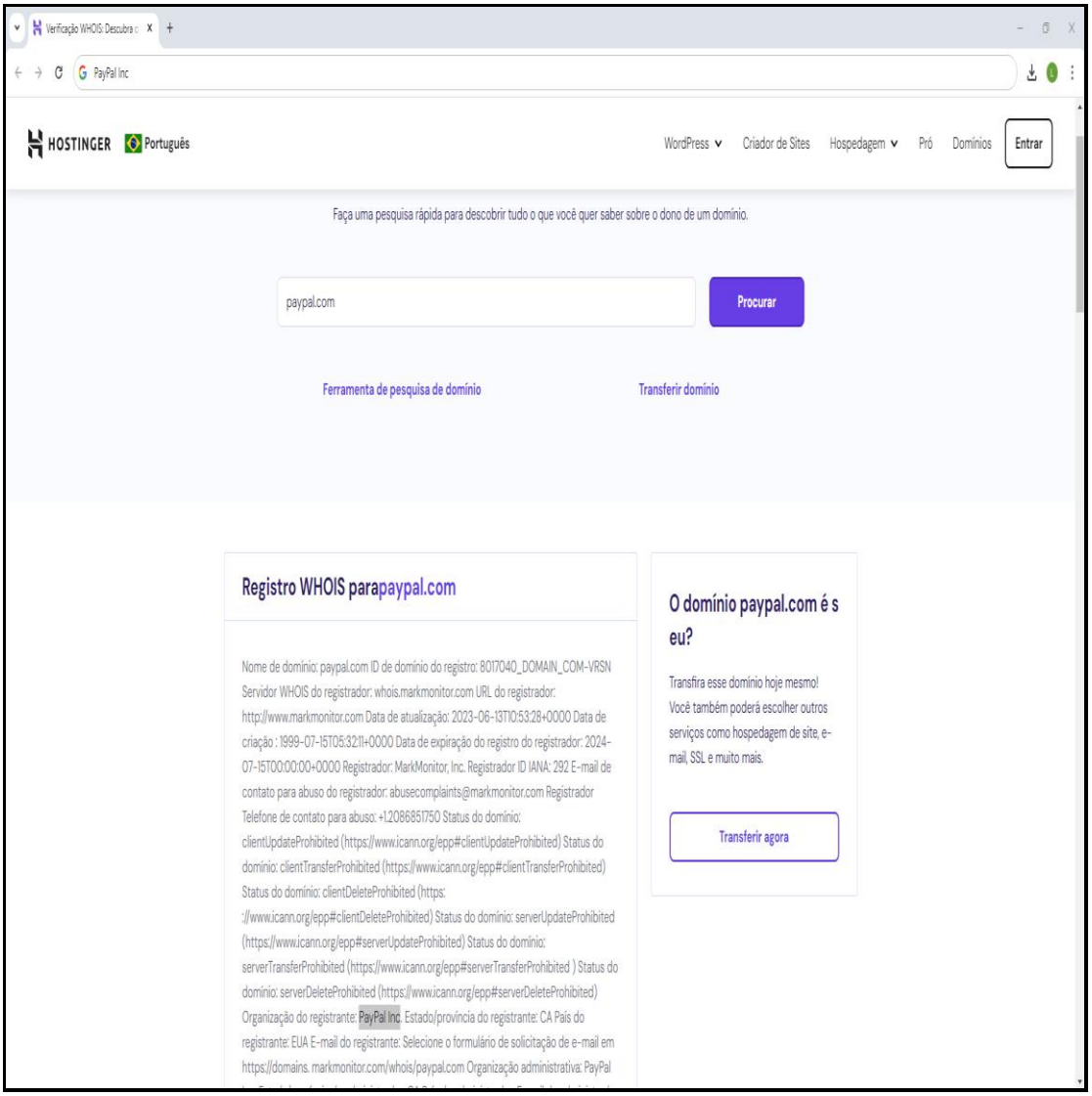
Figura 17 – Utilização da ferramenta WHOIS na pesquisa do domínio kutaukausudahtidakbahagia.online



Fonte: De autoria própria.

Utilizando a mesma ferramenta e realizando a pesquisa pelo domínio paypal.com, pode-se analisar que a ferramenta informa que o nome da organização do registrante do domínio é a PayPal Inc, além de informar diversos dados da empresa demostrando que o domínio é legitimo, conforme apresentado na Figura 18.

Figura 18 – Utilização da ferramenta WHOIS na pesquisa do domínio paypal.com

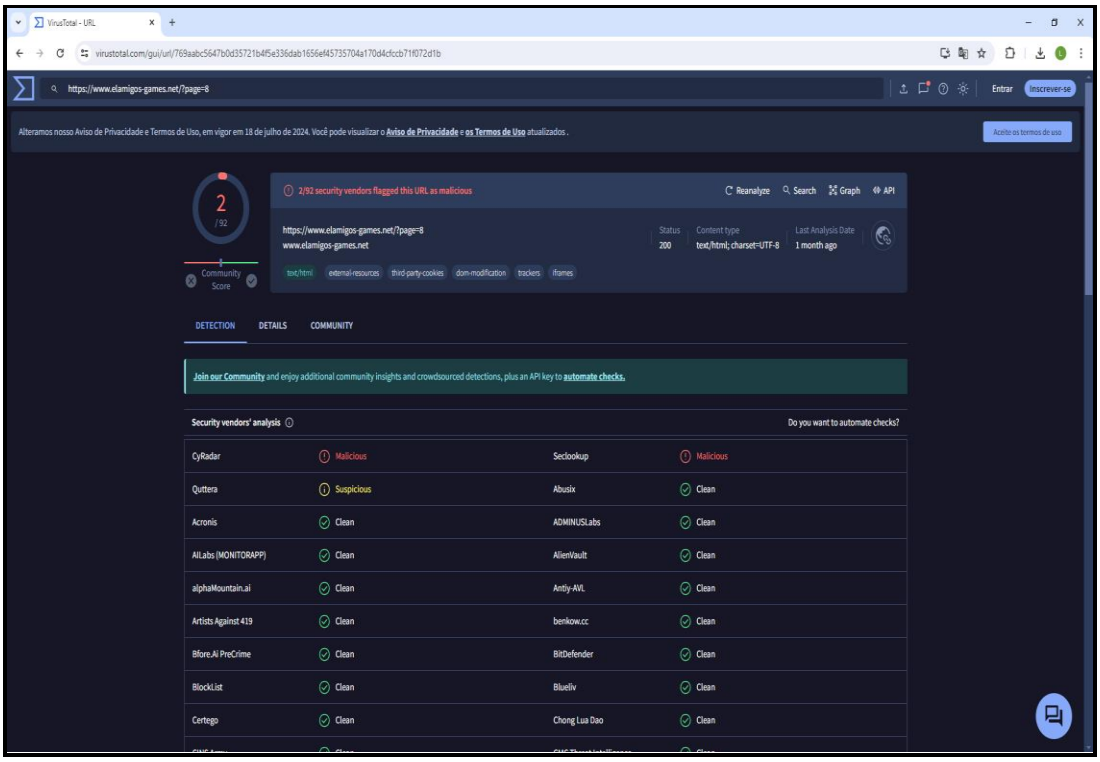


Fonte: De autoria própria.

Realizar uma busca *online* para verificar a reputação do site é essencial. O site como Trustpilot fornecem avaliações e *feedbacks* de usuários sobre o site, podendo ajudar a determinar a confiabilidade do site.

Outra abordagem eficaz é utilizar ferramentas específicas de verificação de segurança. Um exemplo é a ferramenta Virus Total, sendo possível verificar se há relatos de que o site é malicioso. Esta realiza uma pesquisa entre os maiores fornecedores de *softwares* de segurança e fornece um relatório detalhado sobre qualquer ameaça potencial, conforme mostrado na Figura 19.

Figura 19 – Utilização da ferramenta Virus Total na pesquisa do site elamigos-games.net



Fonte: De autoria própria.

No exemplo apresentado na Figura 19, ao pesquisar o site “elamigos-games.net/” é mostrado que algumas empresas de antivírus avaliaram o site como *phishing* ou malicioso.

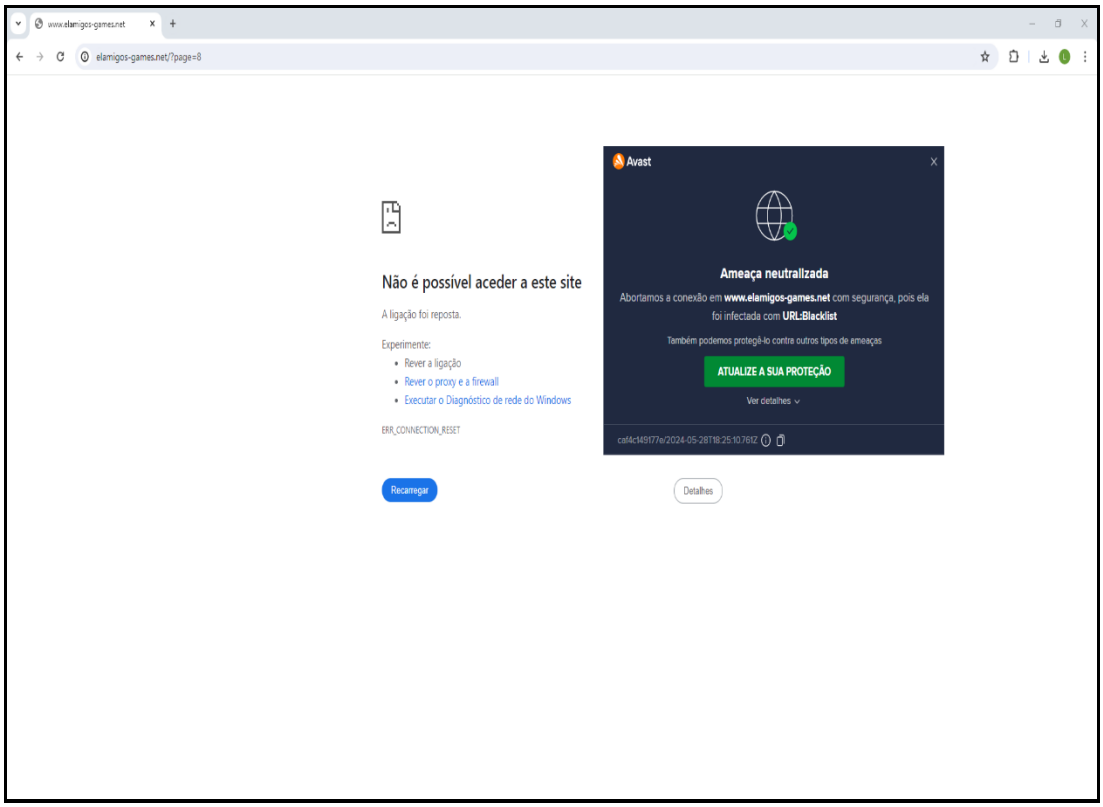
Deve-se utilizar *softwares* antivírus pois, muitos programas antivírus modernos já oferecem proteção avançada contra um ataque cibernéticos, incluindo a capacidade de filtrar *websites* perigosos.

Esses *softwares* analisam o tráfego da Internet em tempo real, identificando e bloqueando sites maliciosos que possam representar uma ameaça à segurança do usuário.

Além disso, eles frequentemente atualizam suas bases de dados de ameaças para garantir uma defesa contínua contra novas formas de *malware* e tentativas de *phishing*.

Utilizando o *software* Avast Antivirus, ao tentar acessar algum site malicioso, o *software* no momento antes de acessar o site identifica e bloqueia o acesso, protegendo o usuário de possíveis ameaças, conforme ilustrado na Figura 20.

Figura 20 – Proteção do antivírus Avast



Fonte: De autoria própria.

Ao tentar acessar o site “elamigos-games.net/”, o antivirus bloqueia o acesso e informa que o site é uma possível ameaça.

A utilização de um antivírus é uma medida essencial para garantir a segurança na navegação de sites web, prevenindo o acesso a conteúdo prejudiciais e protegendo informações o usuário.

Uma medida adicional de segurança para proteger os sites é a implementação de um *firewall*.

Ao adotar um sistema de *firewall*, adiciona-se uma camada extra de proteção ao navegar na web.

O *firewall* atua como uma barreira entre o dispositivo do usuário e a internet, monitorando o tráfego de entrada e saída e filtrando potenciais ameaças. Ele pode

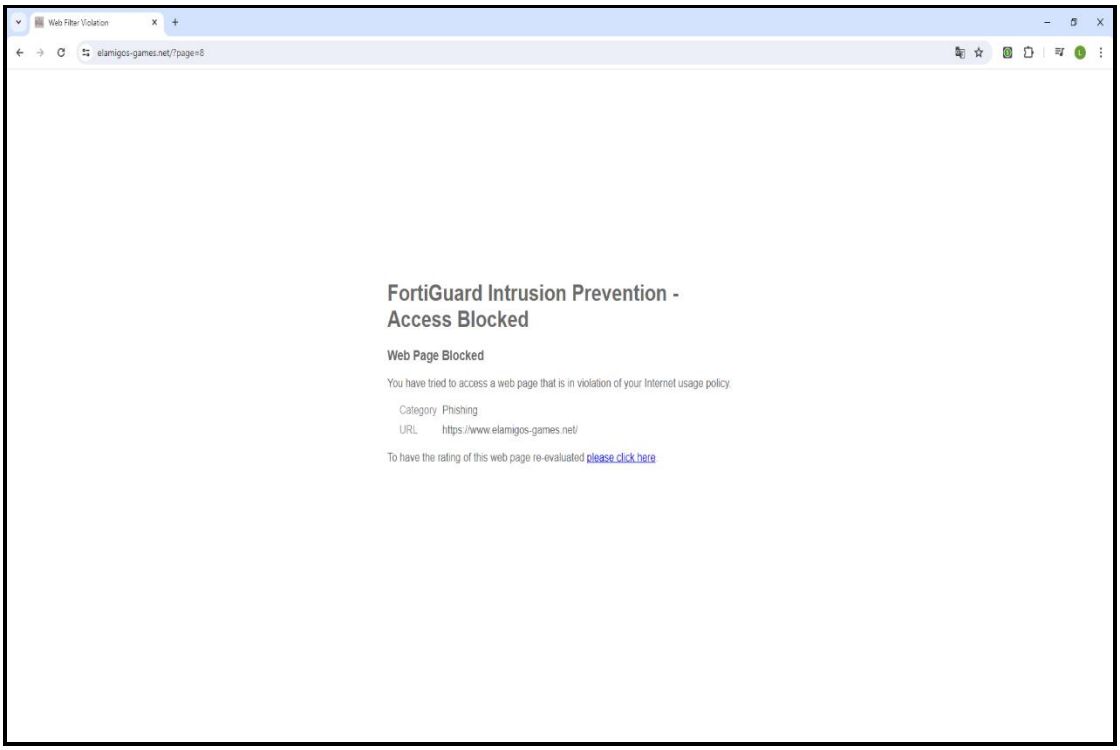
bloquear acessos não autorizados, impedir a entrada de *malware* e até mesmo detectar atividades suspeitas.

Essa defesa proativa é fundamental para salvaguardar informações sensíveis, como dados pessoais e financeiros e garantir uma experiência *online* mais segura e confiável.

Com o *Firewall* Fortinet pode-se visualizar que possui a tecnologia *Filtering Service*.

O *FortiGuard URL Web Filtering Service* oferece proteção contra ameaças abrangente para lidar com ameaças, incluindo *ransomware*, roubo de credenciais, *phishing*, spam e outros ataques transmitidos pela Web. Ele usa análise de comportamento orientada por IA e correlação para bloquear URLs mal-intencionados desconhecidos quase imediatamente, com falsos negativos quase zero (Fortinet, 2024).

Figura 21 – Proteção do *Firewall* Fortinet



Fonte: De autoria própria.

Ao tentar acessar o site “elamigos-games.net/”, o firewall realizar o bloqueia do site e informa ao usuário que o site está classificado com *phishing*.

5.1.2 CONSCIENTIZAÇÃO E TREINAMENTO PARA OS USUÁRIOS

Outra abordagem para manter um ambiente mais seguro contra-ataques é a conscientização e treinamento para os usuários.

“A conscientização sobre engenharia social envolve educar as pessoas sobre as táticas e técnicas usadas pelos golpistas e criminosos cibernéticos que se aproveitam da confiança, manipulação emocional e persuasão para obter acesso não autorizado a informações confidenciai.” (Helena, 2023).

Esta prática envolve educar os funcionários sobre as ameaças cibernéticas, os sinais de possíveis ataques e as medidas preventivas que podem ser adotadas para proteger os dados.

Ao fornecer treinamento sobre segurança da informação e realizar simulações de ataques de *phishing*, os usuários podem se tornar mais eficientes na identificar de um ataque, assim podendo relatar atividades suspeitas.

5.1.3 CARTILHA DE SEGURANÇA

Cartilha de segurança é um documento projetado para educar os usuários sobre boas práticas de seguras, com o objetivo promover a conscientização sobre os riscos no ambiente virtual e evitar incidentes de segurança.

O Centro de estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (CERT.br) possui uma cartilha de segurança gratuita para estudo. “Os materiais contêm recomendações e dicas para aumentar a sua segurança e se proteger de possíveis ameaças” (CERT.br, 2024).

“A Cartilha de Segurança para Internet é um documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças.” (Comite Gestor da Internet no Brasil, 2012).

Nas documentações gratuitas são encontradas diversas tópicos de proteção como, Segurança na Internet, Golpes na Internet, Ataques na Internet, Códigos maliciosos (Malware), Spam, Outros riscos, Mecanismos de segurança, Contas e senhas, Criptografia, Uso seguro da Internet, Privacidade, Segurança de computadores, Segurança de redes e Segurança em dispositivos móveis.

Uma cartilha de segurança desempenha um papel crucial na educação e conscientização dos usuários nas boas práticas de segurança cibernética, sendo um método eficaz na prevenção de possíveis ataques cibernéticos.

5.2 METODO DE PREVENÇÃO AO *PHISHING*

Como citado no capítulo 4, existem diversas variações de um ataque de *phishing*, e a diferença de cada ataque é o meio de comunicação utilizado no ataque e escolha da vítima. Para mitigar um ataque de *phishing* é necessário validação rigorosamente o meio de comunicação.

É muito comum pessoas com menos familiaridade com tecnologia acabarem caindo em ataques de *phishing*.

Ao receber uma mensagem suspeita, independente do meio de comunicação, deve ser analisado de forma paciente e no caso de dúvidas sobre a autenticidade da mensagem, deve-se entrar em contato com a suposta entidade através de um canal de comunicação oficial.

Ao adotar uma abordagem cautelosa e diligente, é possível proteger-se contra essas ameaças e manter-se seguro no ambiente *online*.

Outra medida de segurança crucial a ser adotada é a utilização do duplo fator de autenticação. O duplo fator ou 2FA, é um sistema de segurança que ao tentar realizar login em alguma aplicação, é exigido além da senha uma segunda forma de autenticação, como, código enviado para um dispositivo móvel cadastrado ou confirmação via aplicativo.

Essa medida de segurança é altamente eficaz na prevenção da perda de acesso à conta em caso de um ataque bem-sucedido. Mesmo que o usuário caia em um golpe de *phishing* e divulgue seus dados de login, o invasor ainda encontrará uma barreira adicional.

É essencial que os usuários prestem total atenção ao processo de autenticação de dois fatores, pois os golpistas frequentemente empregam métodos de *phishing* para enganar os indivíduos, solicitando a realizar da segunda etapa da autenticação.

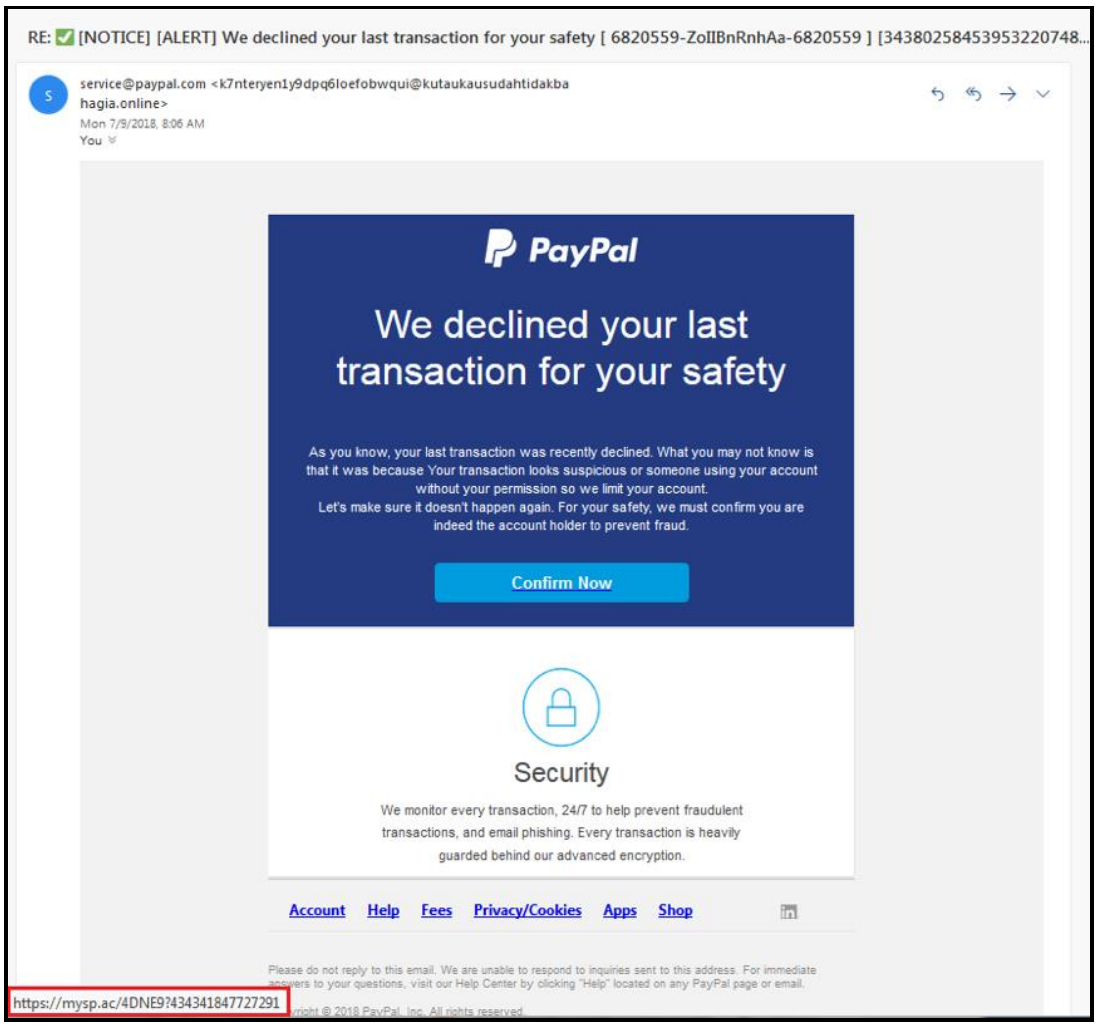
5.2.1 METODOS DE PREVENÇÃO AO ATAQUE *PHISHING* POR E-MAIL

Para prevenir-se de um ataque de *phishing* por e-mail é necessário de bastante atenção do usuário, alguns métodos de prevenção podem ser utilizados pelo usuário, tais como:

Verificação de e-mails suspeitos, o usuário deve estar sempre atento, e realizar verificações no e-mail, como:

Análise do remetente, sempre ao receber um e-mail deve-se verificar o remetente, o endereço é constituído por nome do e-mail após o domínio, o nome do e-mail fica localizado antes do caractere “@” e o domínio após.

Figura 22 – Ataque de *phishing* por e-mail



Fonte: Malwarebytes, 2024

Ao analisarmos a Figura 22, domínio do remetente é @kutaukausudahtidakbahagia.online, sendo que o padrão utilizado por empresas é o próprio nome, no caso da empresa Paypal, o domínio oficial é @paypal.com.

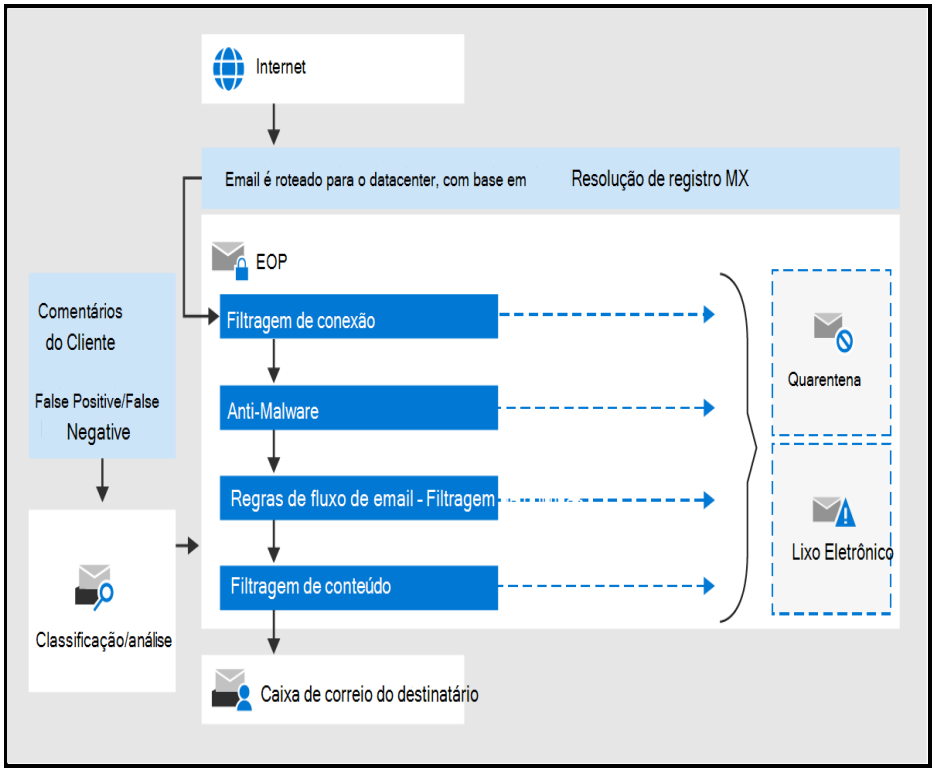
Pode-se observar que em golpes também é utilizado domínios públicos como @gmail.com, @outlook.com, @uol.com.br, entre outros, assim sendo uma forma muito informal que não é utilizado por empresas no envio de informações.

Outra verificação que pode ser realizado para analisar se o e-mail enviado pode ser um ataque de de *phishing* por e-mail é a gramática e redação do e-mail, verificação se estão corretos.

Para mitigar os ataques de *phishing* por e-mail, os gestores do domínio podem implementar práticas de segurança rigorosas, como implementação de monitoramento no tráfego de e-mails, buscando atividades suspeitas de envio e recebimento de dados, filtragem de e-mails, detectando e bloqueando possíveis sinais de *phishing* antes de fechar na caixa de entrada dos usuários, verificação de rigistro de DNS por meio SPF, DKIM ou DMARC, entre outros.

O uso de ferramentas anti-*phishing* é comum entre os fornecedores de e-mail. Geralmente, essas ferramentas são integradas aos serviços de e-mail, como no caso da Microsoft, que oferece a ferramenta *Exchange Online Protection*. “*Microsoft Exchange Online Protection* (EOP) é um serviço de filtragem de email baseado em nuvem que ajuda a proteger sua organização contra spam e *malware* e inclui recursos para proteger sua organização contra violações de política de mensagens.” (Microsoft, 2023). Quando uma mensagem é recebida pela EOP, ela passa por várias etapas de filtragem. Conforme ilustrado na Figura 23.

Figura 23 – Etapas de proteção do EOP



fonte: Microsoft, 2024

Primeiro, é feita uma verificação da reputação do remetente durante a filtragem de ligação, onde a maioria do spam é interceptada e rejeitada (Microsoft, 2024).

Em seguida, a mensagem é inspecionada em busca de *software* maligno; se encontrado, a mensagem é colocada em quarentena. A filtragem de políticas avalia a mensagem em relação a regras específicas do fluxo de correio criadas pelo administrador (Microsoft, 2024).

Em organizações locais com determinadas licenças, verificações de Prevenção de Perda de Dados (DLP) também são realizadas. Posteriormente, a mensagem passa pela filtragem de conteúdo, onde é classificada como spam, *phishing*, ou *spoofing*, e ações são tomadas com base nessas classificações, como colocar em quarentena ou mover para a pasta de lixo eletrônico.

Os administradores têm controle sobre as políticas de quarentena e configurações relacionadas (Microsoft, 2024).

5.2.2 METODO DE PREVENÇÃO AO ATAQUE *SMISHING*

Para evitar um ataque de *smishing*, pode ser adotado algumas verificações de prevenção.

Verificação o número do remetente, a maioria dos ataques de *smishing* é realizado através de um número convencional (L*ong Numbe*r). As operadoras disponibilizam sistema de *Short Codes*, o *Short Code* são número pequenos de 5 a 6 números que possibilita o envio de SMS. São utilizados para campanha de marketing, notificações entre outros.

Ao verificar o remetente, caso o número seja um *Long Number* é de se suspeitar que seja uma tentativa de ataque, pois empresas em geral não utilizam *Long Number* no sistema de SMS.

Os atacantes já possuem ciência que pode ser suspeito utilizar um *Long Number* em seus ataques, então alguns já utilizam *Shot Code* para realizar o ataque.

Sempre ficar atento aos *links* ou números suspeitos, muitos ataques utilizam o SMS somente como ferramenta para capturar o usuário para outra aplicação, é na maioria dos casos, os golpistas solicitam o usuário a entrar em um *link* ou entrar em contato com um número.

É essencial sempre analisar os *links* e números suspeitos antes de interagir com eles, a fim de evitar possíveis tentativas de ataques. Se houver qualquer dúvida ou suspeita quanto à autenticidade da mensagem recebida, é recomendável que o usuário utilize um canal de comunicação oficial.

5.2.3 METODO DE PREVENÇÃO AO ATAQUE *PHARMING*

Para se proteger contra um ataque de *pharming* deve-se manter uma postura cautelosa e atenta diante de qualquer atividade *online* suspeita.

Desenvolver um senso crítico em relação a ofertas mirabolantes e pedidos inusitados, mesmo quando aparentemente provenientes de fontes confiáveis, como amigos ou familiares.

Ao em vez de aceitar quais solicitações de forma precipitada, é recomendável verificação de autenticidade por meio de comunicação direta, assim confirmando a identidade ou análise detalhada da situação. Essa prática cautelosa não apenas

protege contra potenciais ataques de *pharming*, mas também ajuda na defesa contra outras formas de golpes e fraude.

A implementação do duplo fator de autenticação (2FA), como mencionado anteriormente, desempenha um papel na proteção dos dados e contas dos usuários. Essa camada de proteção adicional de segurança cria uma barreira extra para impedir acessos não autorizados, exigindo ao usuário não apenas a senha, mas também uma segunda forma de verificação, como um código enviado por mensagem de texto ou confirmação no aplicativo de autenticação.

Ao utilizar 2FA, o risco de invasões reduz é reduzido, assim não comprometendo o acesso aos dados sensíveis, garantindo assim uma proteção para os usuários.

É crucial utilizar os métodos previamente demonstrados para validação de sites e conscientização dos usuários. A verificação da autenticidade dos domínios visitados, utilização do duplo fator de autenticação e conscientização do usuário, torna o ambiente de navegação mais seguro.

5.2.4 METODO DE PREVENÇÃO AO ATAQUE *VISHING*

Para se proteger de um ataque de *vishing*, os usuários devem ter bastante atenção ao receber qualquer tipo de ligação.

O usuário deve realizar a verificação do número do chamador. Se o número não estiver registrado em seus contatos ou não for reconhecido, o usuário deve proceder com cautela, pois isso pode indicar uma possível ataque de *vishing*.

É fundamental estar atento a qualquer solicitação incomum de números ou informações pessoais por parte do chamador.

Caso houver qualquer indício de que a ligação possa ser de um ataque de *vishing*, o usuário deve tomar medidas adicionais de proteção, como recusar fornecer informações, encerrar a ligação e entrar em contato por um canal de comunicação legitimidade.

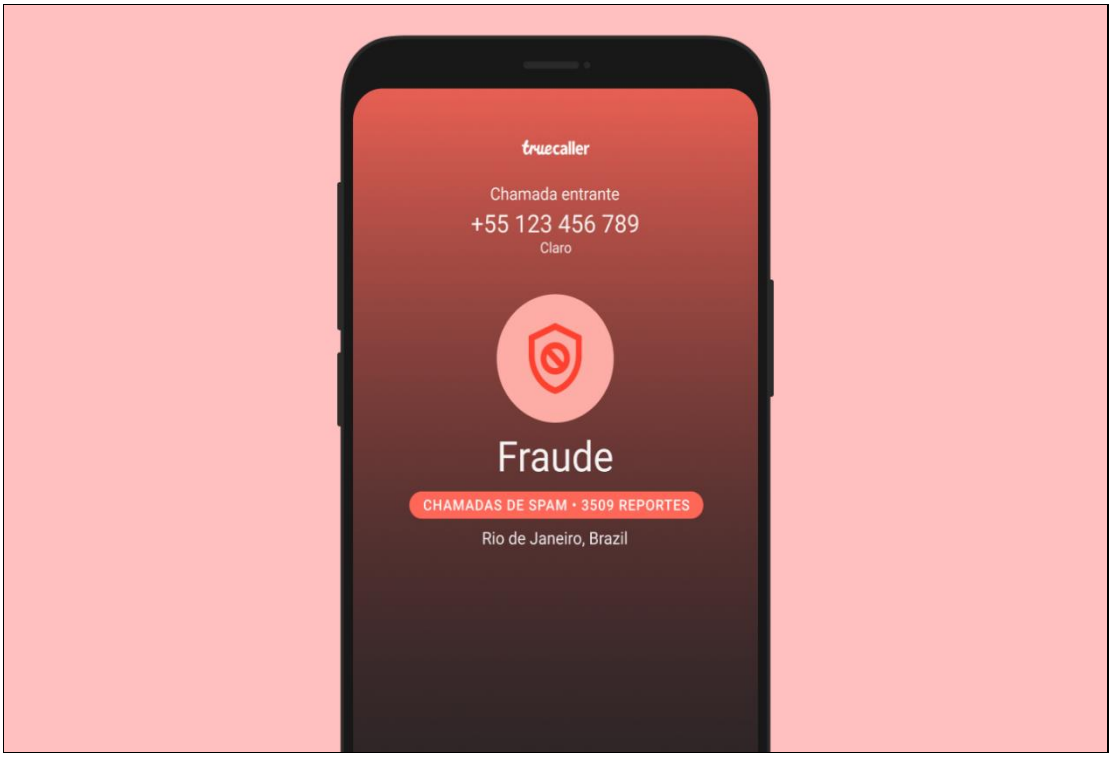
Outra ferramenta essencial para proteção aos ataques de *vishing* são as soluções de controle e monitoramento de chamadas. Essas ferramentas oferecem uma defesa eficaz ao permitir que os usuários monitorem e controlem as chamadas recebidas, identificando rapidamente possíveis tentativas de *vishing*.

Ferramenta de monitoramento de chamado oferecem recursos avançados, como bloqueio de chamadas indesejadas e filtragem de spam, fortalecendo ainda mais a segurança das comunicações telefônicas e reduzindo o risco de cair em golpes de *vishing*.

Uma desta ferramenta é a TrueCaller, a ferramenta oferece uma tecnologia de deteção de possíveis números que realizam ataques de *vishing*.

“O aplicativo identifica automaticamente chamadas realizadas por robôs, golpes, fraudes, assédio. O banco de dados internacional de remetentes de spam, que são reportados por nossos usuários, está disponível para qualquer pessoa que use o TrueCaller para ajudar a reduzir o ruído de números indesejados.” (TrueCaller, 2024), conforme ilustrado na Figura 24.

Figura 24 – Sistema de proteção TrueCaller



Fonte: TrueCaller, 2024.

Ao utilizar a soluções de controle e monitoramento de chamadas proporciona ao usuário segurança contra ataques de *vishing*.

Essa postura ajuda a mitigar os riscos de cair em golpes de *vishing* e a proteger a segurança e privacidade do usuário.

5.3 METODO DE PREVENÇÃO AO ATAQUE *BAITING*

Para proteger-se contra um ataque de *baiting*, é possível adotar diversas medidas de segurança.

Uma das principais maneiras de se tornar vítima de um ataque de *baiting* é por meio do *download* de *softwares* de origem duvidosa, como propagandas suspeitas, sites não confiáveis e por meio da pirataria, entre outros.

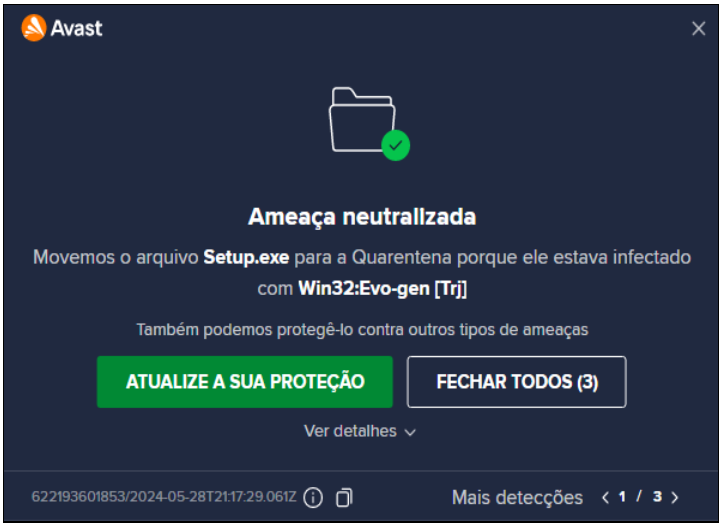
Esses *downloads* de origem duvidosa servem como portas de entrada para os atacantes, que podem injetar *malware* ou enganar os usuários para revelar informações sensíveis. Portanto, é de extrema importância que, ao realizar qualquer *download*, os usuários verifiquem cuidadosamente a origem do *software* para garantir sua legitimidade e segurança.

Também é de suma importância a implementação de sistema antivírus, ao utilizar um antivírus, você adiciona uma camada de proteção robusta contra uma ampla gama de ameaças cibernéticas, incluindo instalações clandestinas de vírus.

O programa Avast Antivirus detecta, bloqueia e remove todos os tipos de *malwares*: vírus, *adwares*, *spywares*, cavalos de Troia e muito mais.” (Avast, 2024).

Quando um *software* malicioso é detectado durante a tentativa de instalação, o antivírus Avast conduz uma análise imediata. Caso seja identificado algum tipo de *malware* no arquivo executável, o Avast prontamente bloqueia e elimina a ameaça. Esse processo é exemplificado na Figura 25.

Figura 25 – Proteção do antivírus Avast



Fonte: De autoria própria.

Essa medida protetiva não apenas ajuda a preservar a integridade de seus dados e dispositivos, mas também oferece tranquilidade ao navegar na internet e interagir com arquivos de origens diversas.

Ao utilizar dispositivos de armazenamento removíveis, como *pendrives*, HDs externos, entre outros, é fundamental realizar uma verificação minuciosa em busca de *malware* antes de acessar qualquer arquivo.

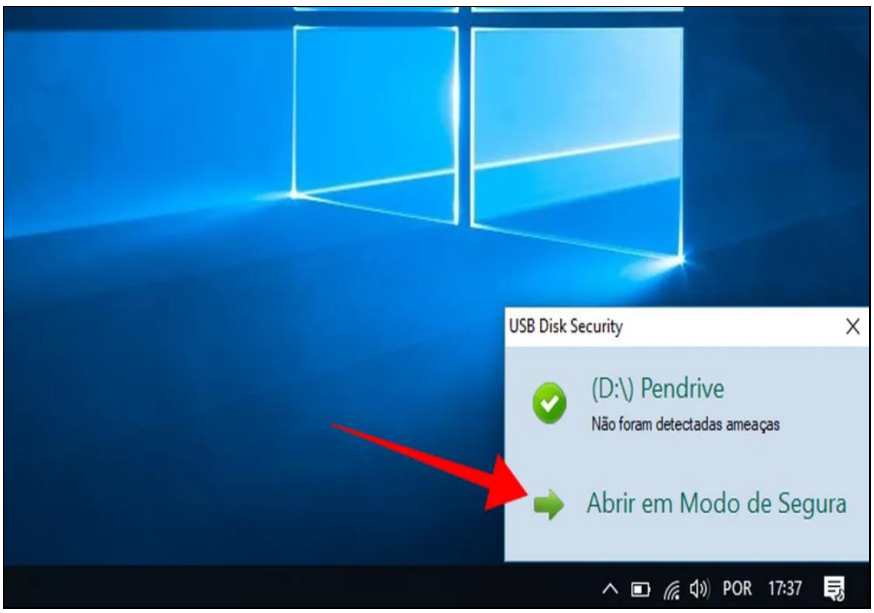
Os dispositivos podem ser potenciais para a propagação de *malware*, pois podem ser infectados por meio de computadores não seguros ou pela transferência de arquivos de fontes.

Para verificar a integridade de um dispositivo móvel, pode-se utilizar *softwares* de verificação, como USB Disk Security.

“USB Disk Security trabalha na prevenção de *malwares* do tipo “*autorun*”, executados de forma automática quando o dispositivo é conectado via USB. Ele verifica regularmente os dispositivos de armazenamento USB recém-inseridos e limpa potenciais ameaças.” (Alves, 2018).

“Ao conectar um *pendrive* na porta USB, o *software* faz uma varredura automática e mostra, em uma notificação, se existe alguma ameaça. Ao clicar no *pendrive* para acessar os arquivos ou opte pelo “Modo seguro” para abrir com cautela em um ambiente protegido.” (Alves, 2018).

Figura 26 – Sistema de proteção USB Disk Security



fonte: Alves, 2018

Essa prática simples, ajuda a mitigar os riscos de infecção por *malware* e protege a segurança de seus dispositivos e dados.

5.4 METODO DE PREVENÇÃO AO ATAQUE *TAILGATING*

O ataque *tailgating* é geralmente voltado para o ambiente empresarial e pode trazer diversos prejuízos, tanto financeiros quanto de reputação.

A forma mais eficaz de prevenção é utilização de rígidas políticas de acesso, como,

Utilização de crachás de identificação, os funcionários devem conter um mecanismo de identificação para entrada, sendo uma medida de controle de entrada e saída dos ambientes supervisionados.

Este controle pode ser realizado tanto por sistema de segurança como portas com leitores de cartão de acesso, leitores de biometria ou leitores faciais, torniquetes, entre outros.

Tecnologias avançadas de vigilância e segurança é fundamental para prevenção de ataques de *tailgating*. Utilizar um sistema de segurança monitorado por vídeo proporciona uma vigilância contínua das entradas e saídas de áreas, permitindo a detecção de qualquer tentativa de acesso não autorizado.

Além disso, a instalação de alarmes de segurança adicionais oferece uma camada extra de proteção, alertando os responsáveis de segurança sobre a presença de indivíduos não autorizados e facilitando a verificação da identidade dos que tentam entrar no local.

Essas medidas combinadas criam um ambiente de segurança robusto e protegido, reduzindo significativamente a probabilidade de sucesso de ataques de *tailgating* e protegendo os ativos e pessoal da organização contra ameaças potenciais.

5.5 METODO DE PREVENÇÃO AO ATAQUE *SCAREWARE*

Os ataques de *scareware*, também conhecidos como "falso alertas", podem ser reduzidos como a utilização de *software* antivírus.

Conforme mencionado anteriormente, um antivírus não apenas identifica e remove ameaças de *scareware*, mas também fornece uma defesa contra variedade de outras formas de *malware*.

Essa ferramenta examina continuamente o sistema em busca de sinais de atividade maliciosa, prevenindo assim que o usuário sofra um ataque de *scareware*.

É suma importância a conscientização sobre esse tipo de ataque e de garantir que os usuários estejam atentos a possíveis tentativas de ataques de *scareware*.

A conscientização e a sensibilização dos usuários são primordiais para capacitá-los a reconhecer e responder adequadamente às ameaças de ataques de *scareware*.

5.6 METODO DE PREVENÇÃO AO ATAQUE *WATERING HOLE*

O ataque de *watering hole* envolve a invasão de um site frequentemente visitado por funcionários de uma organização, com o objetivo de infectar seus dispositivos com *malware*.

Para se prevenir contra ataques de *watering hole*, os usuários devem utilizar *softwares* antivírus, conforme mencionado anteriormente, para evitar a propagação de *malware* em seus dispositivos.

É essencial que os proprietários dos sites tomem medidas de proteção para garantir a segurança de suas aplicações.

Os proprietários de web sites devem manter todos os *softwares*, *plugins* e sistemas de gerenciamento de conteúdo (CMS) do site sempre atualizados com os últimos patches de segurança, assim prevenindo de possíveis vulnerabilidade conhecidas que podem ser utilizadas pelos atacantes.

A implementação de soluções de monitoramento contínuo permite detectar atividades suspeitas no site em tempo real. Ferramentas de monitoramento como Splunk ajudam a identificar tentativas de invasão ou a presença de *malware*, permitindo a visualização de possíveis ameaças.

O Splunk é um *software* que possui um conjunto de serviços que permite a agregar, analisar, transformar, visualizar, compartilhar e realizar diversas outras operações em dados de quaisquer origens, como, computadores, dispositivos de rede, máquinas virtuais, arquivos, mensagens, entre outros (Dirani, 2021).

O uso de firewalls é essencial para bloquear o tráfego malicioso, como mencionado anteriormente.

Realizar auditorias de segurança regularmente é extremamente importante para um ambiente seguro, identificar e corrigir vulnerabilidades faz com que o sistema fique protegido de ataque.

Testes de penetração, simula ataques e revelar pontos fracos no sistema, permitindo que sejam corrigidos antes de serem explorados.

5.7 METODO DE PREVENÇÃO AO ATAQUE *QUID PRO QUO*

Em um ataque de *quid pro quo*, onde um atacante oferece algo em troca de informações ou acesso, pode-se enfrentar dois cenários.

No primeiro cenário, a vítima não tem conhecimento do ataque.

No segundo cenário, há um indivíduo dentro do sistema que está ciente do ataque e colabora com o atacante.

Para prevenir ataques no primeiro cenário, é crucial educar os funcionários sobre práticas de segurança, como a verificação de solicitações incomuns e o cuidado ao compartilhar informações. Além disso, implementar sistemas de monitoramento, como sistemas prevenção contra perda de dados (DLP), Prevenção de Intrusões (IPS), Sistemas de Detecção de Intrusões (IDS) e Soluções de Monitoramento Contínuo de Segurança (CSM), pode ajudar a detectar atividades suspeitas.

No segundo cenário, onde há colaboração de um usuário, é importante realizar verificações de antecedentes rigorosas, promover uma cultura de segurança e implementar controles de acesso rigorosos. Auditorias regulares e sistemas de denúncia anônima também podem ajudar a identificar e mitigar ameaças internas.

5.8 METODO DE PREVENÇÃO AO ATAQUE *OPEN SOURCE INTELLIGENCE*

OSINT refere-se à análise e coleta de informações disponíveis publicamente de um usuário, frequentemente utilizado para conduzir ataques de engenharia social.

Conscientização de publicação de dados pessoas é uma prática de proteção contra um ataque OSINT, a divulgação de dados pessoais ao público pode gerar uma vulnerabilidade, deve ser analisando o que se publica na Internet, muitos dos ataques

vem de informações onde o usuário simplesmente publica uma informação pessoal em suas redes sociais, gerando assim dados para o atacante.

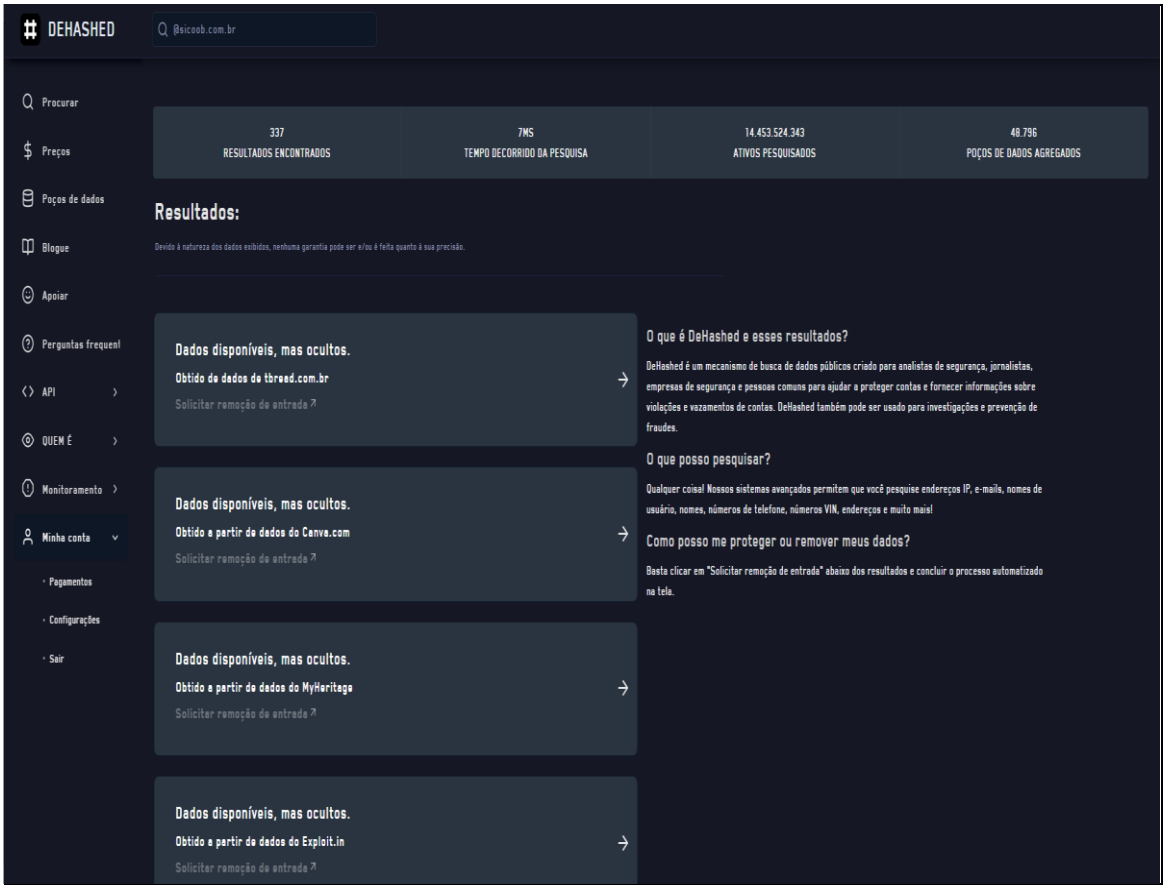
As empresas devem desenvolver e implementar políticas claras sobre segurança da informação que limita a divulgação de dados dentro da empresa, algumas destas políticas são:

Utilização de ferramentas para verificação de vazamento de dados**,** pode-se utilizar a ferramenta DeHashed.

DeHashed é um mecanismo de busca de dados públicos criado para analistas de segurança, jornalistas, empresas de segurança e pessoas comuns para ajudar a proteger contas e fornecer informações sobre violações e vazamentos de contas. DeHashed também pode ser usado para investigações e prevenção de fraudes. (DeHashed, 2024).

Ao realizamos a pesquisa é identificado possíveis ameaças que se encontra públicas na internet, conforme demostrado na Figura 27.

Figura 27 – Sistema Dehashed buscando @sicoob.com.br



Fonte: De autoria própria.

Ao utilizar a ferramenta e realizar a pesquisa, verificamos que a busca por “@sicoob.com.br” resultou em 337 registros. Esses registros podem conter informações ou falhas de segurança que comprometem a empresa. Pode-se analisar os dados disponíveis *online* e neutralizar possíveis ataques.

Utilização de senhas fortes**,** para se defender do OSINT é importante a utilização de senhas fortes, algumas das regras para a senha ser considerada forte são:

- Senha deve que contenha mais de 8 caracteres.
- Senha deve conter letras maiúsculas e minúsculas.
- Senha deve conter caracteres especiais.
- Senha não pode conter sequências de caracteres.
- Senha não deve conter informações pessoas como, nome do filho, datas de nascimento, nome do animal de estimação, entre outros.
- Senha deve ser atualizada a cada 45 dias.

Uma camada de proteção adicional contra este tipo de golpe é o uso de um gerenciador de senhas.

Um gerenciador de senhas armazena e organiza senhas em um cofre criptografado, acessível com uma única senha mestre. Ele gera senhas fortes e únicas para cada conta, reduzindo o risco de reutilização de senhas e facilitando a gestão de credenciais.

Isso aumenta a segurança, pois dificulta a ação dos atacantes que dependem de senhas fracas ou repetidas para realizar ataques.

5.9 METODO DE PREVENÇÃO AO ATAQUE *DUMPSTER DIVING*

O ataque “*dumpster diving*” é prática que envolve a buscar informações confidenciais ou valiosos em resíduos. Embora esse ataque seja mais comum em empresas, também pode ser realizado em usuários convencionais, assim os métodos de prevenção podem ser utilizados para ambos.

É essencial que haja políticas de gerenciamento de documentos, incluindo a implementação de regras específicas para documentos impressos da empresa. Estas políticas devem abranger normas de armazenamento e descarte adequado, garantindo a segurança e a confidencialidade das informações.

Documentos armazenados fisicamente devem ser mantidos em locais seguros e confidenciais, enquanto os documentos para descarte devem ser destruídos.

Utilização de documentos digitais é importante promover a utilização do uso de documentos digital, atualmente é possível assinar e visualizar documentos digitalmente. Devido ao avanço da tecnologia de assinatura digital, que oferece uma maneira segura de autenticar documentos eletronicamente.

Não havendo necessidade de cópias físicas em papel, é mitigado o risco de vazamentos de informações e de um ataque “*dumpster diving*”.

Realizar o descarte correto de equipamentos eletrônicos que armazenam informações sensíveis, como computadores, celulares, impressoras e câmeras de segurança, é fundamental que realize o descarte forma correta.

Antes do descarte, todas as informações devem ser apagadas dos equipamentos e verificado a possibilidade da recuperação dos dados. Simplesmente formatar um dispositivo não é suficiente, pois existem métodos de recuperação de dados que podem restaurar informações mesmo após uma formatação.

No caso de dispositivos como computadores, *notebooks* e smartphones que utilizam um sistema de armazenamento, como discos rígidos ou *hard disk* (HD) ou unidades de estado sólido ou *solid-state drive* (SSD), requerer uma técnica de sobreposição de dados múltipla, esta técnica envolve múltiplas gravações que sobrescrevem dados já existentes na memória.

O objetivo é tornar difícil ou mesmo impossível a recuperação dos dados originais, mesmo com técnicas avançadas de recuperação de dados.

Adotando as medidas demostradas, as empresas e os usuários podem reduzir o risco de exposição de informações sensíveis através do *dumpster diving*.

6 CONCLUSÃO

Este projeto de pesquisa visa responder a seguinte questão: Quais são os tipos de ataques de engenharia social na computação e como se proteger?

O objetivo geral foi o de identificar quais são os tipos de ataques cibernéticos de engenharia social e formas de prevenção.

O estudo permitiu concluir que há diversos tipos de ataques de engenharia social, tais como, *pshising*, *baiting*, *tailgating*, *scareware*, *watering hole*, *quid pro quo*, *open source intelligence* e *dumpster divind*. Na medida em que a tecnologia avança, os ataques de engenharia social tornam-se cada vez mais frequentes. Portanto, é essencial intensificar os esforços na prevenção e conscientização dos usuários sobre essas ameaças, visto que podem causar danos irreversíveis e inimagináveis.

Com a tecnologia cada vez mais presente no dia a dia da população deve-se adotar medidas de segurança para proteção própria. Muitas das falhas sistemáticas se dão ao erro humano, que pode gerar inúmeras consequências.

A conscientização da possibilidade de uma invasão através dos métodos de engenharia social mostra-se essencial para fortalecer o ambiente cibernético e a proteção de dados.

Para continuidade desta pesquisa sugere-se os seguintes trabalhos futuros:

- Estudo de casos de engenharia social em ambientes corporativos.
- Elaboração de técnicas de detecção avançadas de ataques de engenharia social.
- Planos de contingência ao ser uma vítima de um ataque de engenharia social.

REFERÊNCIAS

ALVES, Paulo. **Três dicas para evitar que um pendrive com vírus infecte o PC.** 2018. Disponível em: < https://www.techtudo.com.br/dicas-e-tutoriais/2018/08/tres-dicas-para-evitar-que-um-pendrive-com-virus-infecte-o-pc.ghtml>. Acesso: 15 de mai. 2024.

AMAZON. **O que é segurança cibernética?**. 2023. Disponível em: <https://aws.amazon.com/pt/what-is/cybersecurity/>. Acesso em: 21 ago. 2023.

AMERICANAS. **Ar Condicionado Split High Wall Inverter Electrolux Techno Só Frio 12000 BTUs QI12F/QE12F - 220v**. 2023. Disponível em: <https://www.americanas.com.br/produto/32650438/ar-condicionado-split-high-wall-inverter-electrolux-techno-so-frio-12000-btus-qi12f-qe12f-220v?pfm_carac=ar-condicionado-electrolux&pfm_index=4&pfm_page=search&pfm_pos=grid&pfm_type=search_page&offerId=61a4ee4ad9fd6edeec4b7f83&voltagem=220V&condition=NEW>. Acesso: 18 de nov. 2023.

AVAST. **Avast.** 2024. Disponível em: < https://www.avast.com/pt-br/free-antivirus-download#pc>. Acesso: 18 de abr. 2024.

BERTOLLI, Emilia. **O que é um Whaling Attack?**. 2021. Disponível em: <https://www.varonis.com/pt-br/blog/o-que-e-um-whaling-attack>. Acesso em: 16 ago. 2023.

BLASI, Bruno de. **O que é Urubu do Pix? Veja como funciona golpe que promete dinheiro fácil**. 2023. Disponível em: < https://www.techtudo.com.br/listas/2023/06/o-que-e-urubu-do-pix-veja-como-funciona-golpe-que-promete-dinheiro-facil-edsoftwares.ghtml>. Acesso em: 30 mar. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 31 de ago. de 2023.

BUXTON, Oliver. **O que é um scareware.** 202. Disponível em: <https://www.avast.com/pt-br/c-scareware#:~:text=Esses%20pop%2Dups%20de%20v%C3%ADrus,e%20faz%C3%AA%2Dlas%20baixar%20malware.>. Acesso em: 24 de abr. de 2024.

CANAL CIÊNCIAS CRIMINAIS. **Quem foi Frank Abagnale, criminoso que inspirou o filme 'Prenda-me Se For Capaz'**. 2023. Disponível em: <https://canalcienciascriminais.com.br/historia-golpista-frank-abagnale/>. Acesso em: 30 set. 2023.

CERT.br. **CARTILHA DE SEGURANÇA PARA INTERNET**. 2024. Disponível em: < https://cartilha.cert.br/>. Acesso em: 22 de jun. 2024.

CHECK POINT. **Como a IA identifica conteúdo de phishing**. 2024. Disponível em: < https://www.checkpoint.com/pt/cyber-hub/threat-prevention/what-is-email-security/why-you-must-have-ai-for-email-security/#:~:text=Como%20a%20IA%20identifica%20conte%C3%BAdo%20de%20phishing&text=An%C3%A1lise%20Comportamental%3A%20As%20ferramentas%20de,a%20IA%20detecte%20a%20anomalia.>. Acesso em: 30 de abr. de 2024.

CHECK POINT. **What is a Tailgating Attack?**. 2024. Disponível em: < https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/what-is-a-tailgating-attack/>. Acesso em: 30 de abr. de 2024.

CHEN, Heather. MAGRAMO, Kethleen. **Funcionário de multinacional paga US$ 25 mi a golpista que usou "deepfake" para simular reunião**. 2024. Disponível em: <https://www.cnnbrasil.com.br/internacional/funcionario-de-multinacional-paga-us-25-mi-a-golpista-que-usou-deepfake-para-simular-reuniao/>. Acesso em: 30 de abr. de 2024.

CLARANET. **Ataque man-in-the-middle (Mitm)**. 2023. Disponível em: <https:/br.claranet.com/blog/man-in-the-middle-o-que-e>. Acesso em: 30 set. 2023.

CLEARSALE, **Engenharia Social: o que é, tipos de ataque, técnicas e como se proteger**. 2022. Disponível em: <https://blogbr.clear.sale/engenharia-social-o-que-e-e-como-se-proteger>. Acesso: 29 de nov. 2023.

CNN. **Entenda o que é phishing e como se proteger desse golpe**. 2023. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/phishing/#:~:text=O%20ataque%20phishing%20%C3%A9%20um,fingindo%20ser%20uma%20entidade%20confi%C3%A1vel>. Acesso: 21 de set. 2023.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Cartilha de Segurança para Internet Versão 4.0**. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 22 de jun. 2024.

COMPUGRAF. **NotPetya: Tudo sobre o ciberataque mais devastador da história**. 2020. Disponível em: < https://www.compugraf.com.br/blog/notpetya-tudo-sobre-o-ciberataque-mais-devastador-da-historia/>. Acesso em: 15 de abr. 2024.

CRYPTOID. **Protegendo o elo mais fraco: o papel crucial do fator humano na defesa cibernética**. 2023. Disponível em: <https://cryptoid.com.br/ciberseguranca-seguranca-da-informacao/protegendo-o-elo-mais-fraco-o-papel-crucial-do-fator-humano-na-defesa-cibernetica/>. Acesso: 14 de set. 2023.

DEHASHED. **Dehashed**. 2024. Disponível em: < https://dehashed.com/>. Acesso em: 1 de mar. 2024.

DIRANI, Lucas Ruiz. **Splunk: o que é, como funciona e instalação.** 2021. Disponível em: < https://medium.com/fora-de-assunto/splunk-o-que-%C3%A9-quais-s%C3%A3o-os-seus-componentes-e-guia-de-instala%C3%A7%C3%A3o-796ffe3f05d1>. Acesso em: 19 de mar. 2024.

EXAME. **Após ataque hacker, Renner nega que pagou US$ 20 milhões aos criminosos**. 2024. Disponível em: < https://exame.com/tecnologia/renner-sofre-ataque-de-ransomware-e-sistemas-da-empresa-ficam-fora-do-ar/>. Acesso: 30 de abr. 2024.

FEBRABRAN TECH. **Brasil tem alta de 200% nos ataques de engenharia social em 2020**. 2021. Disponível em: < https://febrabantech.febraban.org.br/temas/seguranca/brasil-tem-alta-de-200-nos-ataques-de-engenharia-social-em-2020>. Acesso: 22 de jun. 2024.

FERREIRA, Yuri. **Brasil é lider de golpes no WhatsApp; conheça principais e saiba como se proteger**. 2023. Disponível em: <https://revistaforum.com.br/brasil/2023/3/25/brasil-lider-de-golpes-no-whatsapp-conhea-principais-saiba-como-se-proteger-133324.html>. Acesso: 12 de nov. 2023.

FERNANDES, Oerton. **O Impacto Global da Engenharia Social e a Importância das Camadas de Proteção**. 2023. Disponível em:<https://www.linkedin.com/pulse/o-impacto-global-da-engenharia-social-e-import%C3%A2ncia-das-msc-com-or/?originalSubdomain=pt>. Acesso em: 10 ago. 2023.

FREDA, Anthony. **O que é um scareware? Como identificar e remover**. 2021. Disponível em: <https://www.avg.com/pt/signal/what-is-scareware>. Acesso: 18 de nov. 2023.

G1. **Golpe do call center: criminosos burlam chamadas telefônicas de bancos para aplicar fraudes**. 2024. Disponível em: < https://g1.globo.com/jornal-nacional/noticia/2024/03/02/golpe-do-call-center-criminosos-burlam-chamadas-telefonicas-de-bancos-para-aplicar-fraudes.ghtml>. Acesso: 1 de abr. 2024.

G1. **Golpes e fraudes por e-mail e telefone disparam no Brasil durante a pandemia**. 2021. Disponível em: < https://g1.globo.com/jornal-nacional/noticia/2021/04/16/golpes-e-fraudes-por-telefone-e-e-mail-disparam-no-brasil-durante-a-pandemia.ghtml>. Acesso: 1 de abr. 2024.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. 6. ed. São Paulo: Editora Atlas Ltda., 2017.

GRAY, Joe. **Practical Social Engineering: A Primer for the Ethical Hacker**. 14/06/2021 ed. No Starch Press, 2021.

HELENA, Andréia. **Conscientização sobre a engenharia social.** 2023. Disponível em: < https://www.linkedin.com/pulse/conscientiza%C3%A7%C3%A3o-sobre-engenharia-social-andreia-helena//>. Acesso em: 20 mai. 2024.

HOSTNET. **Spoofing.** 2024. Disponível em: <https://ajuda.hostnet.com.br/spoofing/>. Acesso em: 30 mai. 2024.

IAMARINO, Atila**. Hackers: Guccifer e engenharia social | Nerdologia Tech**. Disponível em: <https://www.youtube.com/watch?v=y9lAbV5l66Q>. 2021. Acesso: 21 de nov. 2023..

IBM. **O que é engenharia social?**. 2023 Disponível em: <https://www.ibm.com/br-pt/topics/social-engineering>. Acesso em: 16 ago. 2023.

IBM. **O que é segurança cibernética?**. 2023. Disponível em: <https://www.ibm.com/br-pt/topics/cybersecurity>. Acesso em: 28 ago. 2023.

KLUSAITÈ, Laura. **Tailgating: o que é e como funciona?T**. 2023. Disponível em: <https://nordvpn.com/pt-br/blog/o-que-e-tailgating/>. Acesso: 22 de nov. 2023

MALENKOVICH, Serge. **O que é um Ataque Man-in-the-Middle?**. 2013. Disponível em: <https://www.kaspersky.com.br/blog/what-is-a-man-in-the-middle-attack/462/>. Acesso em: 06 nov. 2023.

MALWAREBYTES. **Phishing.** 2024. Disponível em: <https://br.malwarebytes.com/phishing/>. Acesso: 29 de mai. 2024

MEIER, Luiz Fernando Mizael. **ENGENHARIA SOCIAL: ESTUDO DE CASO SOBRE OS RISCOS DE UM ATAQUE EFETUADO POR UM EX-FUNCIONÁRIO**. Monografia - Departamento, da Universidade Tecnológica Federal do Paraná. 2018. Disponível em: <https://repositorio.utfpr.edu.br/jspui/bitstream/1/19429/1/CT_GETIC_VII_2018_07.pdf>. Acesso: 27 de set. 2023.

MICROSOFT. **O que é um ataque cibernético?**. 2023. Disponível em: <https://www.microsoft.com/pt-br/security/business/security-101/what-is-a-cyberattack>. Acesso em: 02 set. 2023.

MICROSOFT. **Visão geral do Exchange Online Protection.** 2024. Disponível em: < https://learn.microsoft.com/pt-br/defender-office-365/eop-about>. Acesso em: 24 mai. 2024.

MINUTO DA SEGURANÇA. **O que é um ataque de watering hole?**. 2021. Disponível em: < https://minutodaseguranca.blog.br/o-que-e-um-ataque-de-watering-hole/#:~:text=Um%20ataque%20watering%20hole%20%C3%A9,local%20de%20trabalho%20do%20alvo.>. Acesso em: 28 abr. 2024.

MORRIS, Mark. **Settlement reached in medical billing records case**. 2014. Disponível em: < https://www.kansascity.com/news/local/article4279093.html>. Acesso em: 10 de mai. 2024.

NADEEM, Mohammad Salma. **Engenharia Social: O que é Whaling?**. 2023. Disponível em: <https://blog.mailfence.com/pt/engenharia-social-whaling/>. Acesso em: 02 nov. 2023.

NITNICK, Kevin D.; SIMON, William L.. **The Art of Deception: Controlling the Human Element of Security**. 1eª. ed. John Wiley & Sons**,** 2003.

OLIVEIRA. Aléx de. **Phishing: como se proteger e não cair no golpe**. 2019. Disponível em: <https://www.lumiun.com/blog/phishing-como-se-proteger-e-nao-cair-no-golpe/>. Acesso em: 26 nov. 2023.

OLIVEIRA. Paulo Henrique Baptista de. **A pirataria e o perigo para sua segurança digital!**. 2019. Disponível em: <https://www.untanglebrasil.com.br/a-pirataria-e-o-perigo-para-sua-seguranca-digital/>. Acesso em: 30 abr. 2024.

QUATROCANTOS. **Fraude. Falso aviso do Banco do Brasil. Phishing scam**. 2015. Disponível em: <https://www.quatrocantos.com/lendas/494_fraude_banco_do_brasil.htm>. Acesso: 21 de nov. 2023.

REZENDE, Renato Teixeira. **Tática de Delivery do Grupo FIN7: BadUSB**. 2022. Disponível em: < https://dciber.org/tatica-de-delivery-do-grupo-fin7-badusb/>. Acesso: 22 de nov. 2023.

ROHR, Altieres. **E-mail enviado 'por você mesmo' aplica golpe com ameaça falsa de divulgação de vídeo íntimo**. 2020. Disponível em: <https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2020/12/31/e-mail-enviado-por-voce-mesmo-aplica-golpe-com-ameaca-falsa-de-divulgacao-de-video-intimo.ghtml>. Acesso: 30 de set. 2023.

RUBINSTEINN, Gabriel. **"Elo mais fraco é o ser humano", diz especialista em segurança cibernética**. 2020. Disponível em:<https://exame.com/future-of-money/cybersecurity/elo-mais-fraco-e-o-ser-humano-diz-especialista-em-seguranca-cibernetica/>. Acesso em: 11 ago. 2023.

SOUZA, Daniele. **[Guia] O que é domínio? Para que serve? Entenda tudo!**. 2022. Disponível em: < https://www.godaddy.com/resources/br/artigos/o-que-e-dominio>. Acesso: 12 de mai. 2024.

TRUECALLER. **Bloqueio de Spam.** 2024. Disponível em: <https://www.truecaller.com/pt-br/spam-blocking>. Acesso: 20 de mai. 2024.

TV CULTURA. **Veja como CRIMINOSOS usam a Inteligência Artificial para aplicar GOLPES**. 2024. Disponível em:< https://www.youtube.com/watch?v=8ahZcpL9eIk&ab_channel=JornalismoTVCultura >. Acesso em: 30 abr. 2024.

WAZLAWICK, R. S. **Metodologia da Pesquisa para Ciência da Computação**. 2ª. ed. [S.l.]: Campus**,** 2014.

WIKIPEDIA. **Ataque Smurf**. 2022. Disponível em: <https:/pt.wikipedia.org/wiki/Ataque_Smurf>. Acesso em: 2 out 2023. 2023.

WIKIPEDIA. **Rubber Ducky**. 2022 Disponível em: <https://pt.wikipedia.org/wiki/Rubber_Ducky>. Acesso em: 14 set. 2023.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 ● Setor Universitário
Caixa Postal 86 ● CEP 74605-010
Goiânia ● Goiás ● Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br ● reitoria@pucgoias.edu.br

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O estudante Leonardo de Moura Alves do Curso de Ciencia da Computação, matrícula 20192002800150, telefone: 62 992916524 e-mail leomoura30310@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado ENGENHARIA SOCIAL: ESTUDO DE ATAQUES E MÉTODOS DE PREVENÇÃO, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto(PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 11 de JUNHO DE 2024.

gov.br Documento assinado digitalmente
LEONARDO DE MOURA ALVES
Data: 22/06/2024 18:49:45-0300
Verifique em https://validar.iti.gov.br

Assinatura do autor: _____

Nome completo do autor: Leonardo de Moura Alves

gov.br Documento assinado digitalmente
SOLANGE DA SILVA
Data: 22/06/2024 18:56:42-0300
Verifique em https://validar.iti.gov.br

Assinatura do professor–orientador: _____

Nome completo do professor-orientador: SOLANGE DA SILVA