UNIVERSIDADE ESTADUAL DO PIAUÍ

CAMPUS DRA. JOSEFINA DEMES

CURSO DE GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO

FRANCISCO ÍTALO DIAS TEIXEIRA

O IMPACTO DAS TÉCNICAS DE ENGENHARIA SOCIAL NA SEGURANÇA CIBERNÉTICA DAS PLATAFORMAS DE *STREAMING* DE ENTRETENIMENTO

FLORIANO

2025

FRANCISCO ÍTALO DIAS TEIXEIRA

O IMPACTO DAS TÉCNICAS DE ENGENHARIA SOCIAL NA SEGURANÇA CIBERNÉTICA DAS PLATAFORMAS DE *STREAMING* ENTRETENIMENTO

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciências da Computação da Universidade Estadual do Piauí, como requisito parcial à obtenção do grau de bacharel em Ciências da Computação.

Orientador: Prof. Me. Danilo Borges da Silva.

FLORIANO

2025

O Impacto das Técnicas de Engenharia Social na Segurança Cibernética das Plataformas de *Streaming* de Entretenimento

Francisco Ítalo Dias Teixeira[1], **Danilo Borges**[1]

[1]Ciência da Computação – Universidade Estadual do Piauí (UESPI)
Floriano – PI – Brasil

franciscoteixeira@aluno.uespi.br, danilo@prp.uespi.br

Abstract. *Streaming platforms, such as Netflix and Spotify, have revolutionized entertainment consumption but also face challenges related to cybersecurity. This study investigated the impacts of social engineering attacks on these platforms, highlighting human vulnerability as a critical issue. Strategies such as multifactor authentication, encryption, and educational campaigns were analyzed, concluding that a combination of technological solutions and user awareness is essential to mitigate digital threats.*
Keywords: *Sreaming Platforms. Cybersecurity. Social Engineering.*

Resumo. *As plataformas de streaming, como Netflix e Spotify, revolucionaram o consumo de entretenimento, mas também enfrentam desafios relacionados à segurança cibernética. Este trabalho investigou os impactos de ataques de engenharia social nessas plataformas, destacando a vulnerabilidade humana como um ponto crítico. Foram analisadas estratégias como autenticação multifator, criptografia e campanhas educativas, concluindo que a combinação de soluções tecnológicas e conscientização é essencial para mitigar ameaças digitais.*
Palavras-chave*: Plataformas de Streaming. Cibersegurança. Engenharia Social. Social Engineering.*

1. Introdução

A engenharia social é uma prática maliciosa que utiliza técnicas de manipulação psicológica para induzir indivíduos a revelar informações confidenciais ou realizar ações prejudiciais, muitas vezes sem perceber. Por sua natureza, esse tipo de ataque explora vulnerabilidades humanas, tornando-se uma das estratégias mais eficazes em cibersegurança. Com o avanço da era digital, o crescimento das plataformas de *streaming* de entretenimento, como Netflix, Amazon Prime Video e Disney+, trouxe mudanças significativas no consumo de mídia, mas também ampliou os riscos associados à segurança de dados. Segundo Venkatesha, Reddy e Chandavarkar (2021), o aumento exponencial do uso dessas plataformas, aliado à sofisticação dos ataques de engenharia social, resultou em uma crescente exposição de informações pessoais e sensíveis dos usuários, evidenciando a necessidade de estratégias de proteção mais robustas.

Além de revolucionar o consumo de entretenimento, a popularização das plataformas de *streaming* também trouxe consigo desafios significativos no campo da segurança cibernética. A crescente sofisticação das técnicas de engenharia social tornou-se um fator crítico nesse cenário, explorando vulnerabilidades humanas de maneira estratégica e

eficaz. Conforme Sun et al. (2019), ataques cibernéticos frequentemente envolvem a exploração de fraquezas específicas, com consequências potencialmente prejudiciais, e a engenharia social destaca-se por sua capacidade de contornar barreiras técnicas e manipular diretamente os indivíduos.

De acordo com um relatório da CyberEdge, cerca de 79% das organizações são vítimas de ao menos um ataque bem-sucedido de engenharia social por ano (Hijji; Alam, 2021). Essa estatística ilustra a urgência de proteger os dados pessoais e financeiros dos usuários em um ambiente onde a interação humana pode ser o elo mais fraco. Como apontado por Krombholz et al. (2015), engenheiros sociais preferem enganar as pessoas por meio de informações cuidadosamente manipuladas, em vez de recorrer a invasões técnicas diretas, o que permite que essas práticas se manifestem de maneiras diversas e muitas vezes imprevisíveis.

Entre os métodos mais comuns de engenharia social destaca-se o *phishing*, no qual invasores enviam e-mails ou criam sites falsos que imitam páginas legítimas, com o objetivo principal de obter ganhos financeiros (Benavides et al., 2020). Nesse tipo de ataque, os usuários são induzidos a fornecer informações confidenciais, como senhas e dados de pagamento, acreditando estar interagindo com um serviço legítimo das empresas de *streaming*. Outra prática frequente é o *baiting*, que explora a curiosidade das pessoas para levá-las a agir impulsivamente, comprometendo sua segurança pessoal (Syafitri et al., 2022). Nesse caso, os cibercriminosos oferecem algo aparentemente atraente, como o download gratuito de um filme ou música, para induzir as vítimas a clicar em *links* maliciosos, expondo-se a riscos adicionais.

Mesmo com a crescente sofisticação das técnicas de engenharia social, grande parte dos ataques ainda se baseia em métodos simples, aproveitando situações rotineiras de interação humana. Como apontam Heartfield e Loukas (2018), o ser humano é frequentemente considerado o "elo mais fraco" na segurança cibernética, uma vez que, mesmo com sistemas de proteção robustos, eles podem ser comprometidos caso os atacantes explorem vulnerabilidades humanas. Nesse cenário de ameaças constantes, a segurança da informação destaca-se como uma estratégia essencial para proteger dados e minimizar os impactos de incidentes cibernéticos (Gomes; Reis; Alturas, 2020). Seu principal objetivo é garantir que as informações estejam acessíveis apenas a indivíduos autorizados, por meio de práticas estratégicas de defesa e monitoramento que previnam a perda de dados e assegurem a continuidade dos negócios.

Ser transparente com os usuários é um passo essencial para fortalecer a confiança nas plataformas de *streaming*. As empresas devem comunicar de forma clara suas políticas de trabalho, segurança e privacidade, assegurando aos usuários que suas informações estão protegidas. Além disso, é fundamental relatar incidentes de segurança e detalhar as medidas corretivas tomadas, demonstrando compromisso com a proteção de dados. Recursos educacionais, como guias, vídeos e dicas práticas, podem ser integrados aos aplicativos para ajudar os usuários a reconhecer e evitar ataques. Adicionalmente, como apontado por Subrayan et al. (2017), a implementação de autenticação multifator é uma solução eficaz para verificar a identidade dos usuários de maneira mais segura do que os métodos tradicionais baseados apenas em nome de usuário e senha.

A contribuição ativa das empresas para a segurança virtual é imprescindível. A

troca de informações entre organizações pode promover uma abordagem colaborativa na proteção de dados, enquanto a aplicação de pesquisas recentes permite que essas plataformas se mantenham atualizadas e um passo à frente das ameaças. Monitorar constantemente os sistemas, identificar padrões de ataque e compreender os métodos de manipulação utilizados pelos invasores são tarefas que exigem não apenas investimento, mas também dedicação contínua. Tais práticas reforçam a resiliência das plataformas, mitigando riscos e protegendo os usuários de ameaças emergentes.

Em síntese, os desafios relacionados à proteção nas plataformas de *streaming* vão desde a falta de investimentos em medidas de segurança mais avançadas até a fragilidade de sistemas e a falta de conscientização dos usuários sobre as ameaças existentes. Este trabalho surge, portanto, da necessidade de compreender como os ataques de engenharia social afetam diretamente a segurança desses serviços, destacando a urgência em resolver as vulnerabilidades presentes nesses ambientes digitais. O objetivo desta pesquisa é categorizar as técnicas de engenharia social empregadas contra organizações de entretenimento, avaliar os impactos desses ataques na segurança virtual e examinar as medidas de proteção atualmente utilizadas, contribuindo para um futuro mais seguro para as plataformas e seus usuários.

Na sequência, este trabalho se divide em seções e subseções que estruturam e desenvolvem o tema. A Seção 2 apresenta os trabalhos relacionados com uma revisão de metodologias que investigam incidentes de engenharia social. Na Seção 3, está descrito o processo de revisão em quatro partes: métodos para atacar a engenharia social (Seção 3.1); análise dos métodos e das vantagens na prevenção dos ataques de engenharia social (Seção 3.2); conclusão e discussão sobre os métodos utilizados (Seção 3.3); e métodos propostos pelas plataformas de *streaming* contra a engenharia social (Seção 3.4). Por fim, na Seção 4, é feito um resumo e conclusão do trabalho.

2. Trabalhos Relacionados

Nesta seção é apresentada uma revisão das metodologias aplicadas em estudos que investigam incidentes de segurança relacionados à engenharia social. A análise abrange as técnicas de ataque mais comuns, além de avaliar as medidas de segurança atualmente implementadas para enfrentá-las. A partir da revisão dos trabalhos existentes, busca-se uma compreensão mais profunda das práticas adotadas no campo da segurança da informação, ressaltando a importância de abordagens eficazes para mitigar os riscos associados à engenharia social.

Kumar, Chaudhary e Kumar (2015) trabalham o conceito de engenharia social, que tem como característica a manipulação psicológica de pessoas para obter informações confidenciais. O estudo descreve várias técnicas de ataque, mostrando tanto métodos baseados em interação humana quanto os baseados em computadores. Além disso, o texto discute formas para prevenir esses ataques, tendo como exemplos: a educação e conscientização dos funcionários, a criação de políticas de segurança e a auditoria de práticas empresariais. O artigo conclui que, embora ferramentas de segurança sejam importantes, o elo mais vulnerável é o comportamento humano, reforçando a necessidade de treinamento contínuo para mitigar riscos.

Segundo Adewole, Durosinmi e Polyetchnic (2015) invasores utilizam as fraquezas humanas, para acessar sistemas e roubar dados. A engenharia social pode ocorrer de

duas formas essenciais: por meio de fraudes tecnológicas ou pela manipulação direta de pessoas. Exemplos de fraudes: golpes de *phishing* e enganações por telefone, com os atacantes se passando por figuras de autoridade. Os autores destacam também a importância de criar uma cultura de segurança organizacional, com treinamentos e utilização de ferramentas tecnológicas para evitar esses ataques. A conclusão reforça que, a conscientização e a vigilância dos colaboradores são essenciais para proteger as organizações.

O estudo de Mouton, Leenen e Venter (2016) analisa ataques de engenharia social, destacando o ser humano como o elo mais fraco na segurança da informação, suscetível a manipulações que levam à revelação de dados privados. Os autores categorizam o ataque em seis etapas: formulação do ataque, coleta de informações, preparação, desenvolvimento de relacionamento, exploração do relacionamento e *debriefing*. Esta última etapa refere-se ao processo em que a vítima, após a manipulação, é retirada da situação, permitindo uma análise da operação para verificar se o objetivo foi alcançado.

Ainda no trabalho de Mouton, Leenen e Venter (2016), os autores apresentam modelos de ataques baseados em exemplos reais, o que possibilita aos pesquisadores realizar comparações com modelos de detecção de forma segura e repetível. Esses tipos de ataque evidenciam a sutileza das técnicas empregadas. Em sua conclusão, os autores enfatizam a necessidade de pesquisas futuras, que incluem o desenvolvimento de materiais de conscientização e novos modelos de detecção de ataques, visando aumentar a vigilância contra esses tipos de golpes.

Neupane et al. (2018) expuseram a vulnerabilidade de indivíduos com Transtorno do Espectro Autista (TEA) a ataques de *phishing*, e os comparou com pessoas sem essa condição. A pesquisa, envolveu 15 participantes de cada grupo, testando a capacidade de distinguir entre sites reais e falsos. Apesar da hipótese no começo, que os indivíduos com TEA seriam mais vulneráveis devido aos desafios relacionados ao transtorno, os resultados mostraram que eles não foram mais vulneráveis a golpes de *phishing* do que os demais participantes. Ambos os grupos conseguiram identificar com sucesso sinais de fraude, como a ausência de certificados de segurança e URLs suspeitas, contrariando as expectativas do estudo.

O trabalho de Aldawood e Skinner (2019) destaca a criatividade dos criminosos para táticas de roubo de dados e como é explorado as soluções de conscientização e treinamento para enfrentar ameaças de engenharia social. Com o maior foco nas práticas corporativas, identificando métodos eficazes de treinamento contra os ataques. Ao longo dos tempos, essas metodologias passaram a evoluir para os cenários virtuais, competições, jogos sérios e simulações, contendo experiências imersivas em ameaças reais, permitindo que os participantes aprendam estratégias de mitigação em ambientes controlados, como laboratórios virtuais e torneios.

Em Nakamura e Dobashi (2019), o *phishing* é dito como uma técnica amplamente utilizada para roubo de informações por meio de sites falsos. O artigo mostra uma nova abordagem para combater essa ameaça, a detecção proativa. Essa detecção foca na descoberta de sites de *phishing* de hora zero, que é um site de *phishing* que não foi percebido ainda. Essa abordagem prevê prováveis nomes de domínio que foram falsificados e são relacionados a marcas conhecidas, acessa esses sites, e avalia suas características, pontuando o risco de serem fraudulentos. O método foi eficaz ao detectar sites disfarçados

como *eBay*, Google e Amazon, mostrando sua utilidade ao identificar esses sites rapidamente, possibilitando sua remoção em tempo hábil.

Uma investigação foi feita por Watson et al. (2020) acerca de como é feita a tomada de decisões sobre segurança e privacidade quando se compartilha recursos digitais, como contas de *streaming*. O estudo promoveu entrevistas semiestruturadas com nove grupos e um diário de quatro semanas para compeender como as experiências compartilhadas influenciam nas atitudes individuais. Foi descoberto que as estratégias de proteção foram baseadas de acordo com implícitos e responsabilidades individuais, sem comunicação sobre segurança, resultando em oportunidades desperdiçadas. O trabalho destaca o desejo de criar controles para a segurança cibernética que melhore as dinâmicas sociais desses grupos.

No trabalho de Li et al. (2021), os autores tratam do crescimento das plataformas de transmissão ao vivo no comércio digital e seus desafios por fraudes associadas, sempre envolvendo transações falsas. Eles pontuam que os modelos antifraude tradicionais não fazem mais efeito nesse contexto, devido à natureza heterogênea das redes dessas plataformas, que conectam diversos usuários, *streamers* e produtos. Para resolver esse problema, os autores propuseram a abordagem *LIFE*, que usa uma rede neural de gráfico heterogênea capaz de explorar dados diversos dessas plataformas. Ou seja, o *LIFE* incorpora um algoritmo que propaga rótulos para lidar com a limitação de transações fraudulentas. Os resultados experimentais que foram apresentados mostram que a abordagem utilizada superou outros modelos na detecção de fraudes e na identificação de comunidades fraudulentas em plataformas de comércio digital com transmissão ao vivo.

Em Mallick e Nath (2024) é mostrado como a Internet, que foi criada para comunicação e compartilhamento de informações, foi rapidamente transformada, trazendo desafios à segurança cibernética. Sendo a mesma essencial para proteger a integridade, confidencialidade e disponibilidade de dados e ativos digitais. O estudo faz uma análise sobre os fundamentos da segurança cibernética, suas ameaças atuais e as soluções preventivas. Destaca como vulnerabilidades em protocolos de redes podem ser exploradas por *hackers*. Além disso, a pesquisa também acrescenta a importância de medidas como criptografia e autenticação. Propondo uma análise detalhada das ameaças cibernéticas e soluções para lidar com elas.

Pode-se observar nestes trabalhos que a falta de comunicação sobre segurança leva a oportunidades desperdiçadas na proteção cibernética. Esses resultados ilustram a complexidade dos ataques de engenharia social e a necessidade contínua de pesquisa e formação em segurança da informação, enfatizando a vulnerabilidade humana como um fator crítico a ser abordado.

3. Processo de Revisão

A execução da revisão sistemática de literatura ampla teve a finalidade de delinear o conhecimento existente no campo de investigação sobre ataques de engenharia social que ameacem as organizações de fluxo de mídia. O foco principal da revisão foi verificar os tipos de ataques e soluções de conscientização praticadas nas instituições. A pesquisa foi feita em várias bases de dados como: IEEE Explore, ACM Digital Library e Google Scholar, usando as seguintes palavras-chaves: “Engenharia Social”, “Técnicas de Engenharia Social”, “Cibersegurança” e “Plataformas de *Streaming*”. Foram considerados artigos

com uma ou várias palavras-chave e um critério temporal de 10 anos, de 2014 a 2024.

A pesquisa resultou em um total de 4.113 artigos distríbuidos entre as bases de dados: 7 artigos no IEEE Explore, 1.626 no ACM Digital Library e 2.480 no Google Scholar. Após a aplicação de critérios de relevância e filtragem inicial (análise de títulos e resumos), 3.920 artigos foram excluídos por não se alinharem diretamente ao tema de ataques de engenharia social ou por não apresentarem soluções específicas para conscientização em plataformas de *streaming*. Restando apenas 193 artigos que estão relacionados com o tema. Sendo 2 artigos no IEEE Explore, 31 no ACM Digital Library e 160 no Google Scholar. Dos 193 artigos relacionados ao tema, apenas 22 foram utilizados no trabalho após uma análise qualitativa, que avaliou a profundidade do conteúdo, o alinhamento com os objetivos do estudo e a qualidade da pesquisa.

O refinamento é detalhado na Figura 1, que ilustra o total de artigos inicialmente encontrados, o total de artigos que restaram após a triagem inicial, a distribuição da quantidade de artigos em cada base de dados e o número de artigos selecionados para fazer parte do trabalho após análise qualitativa.

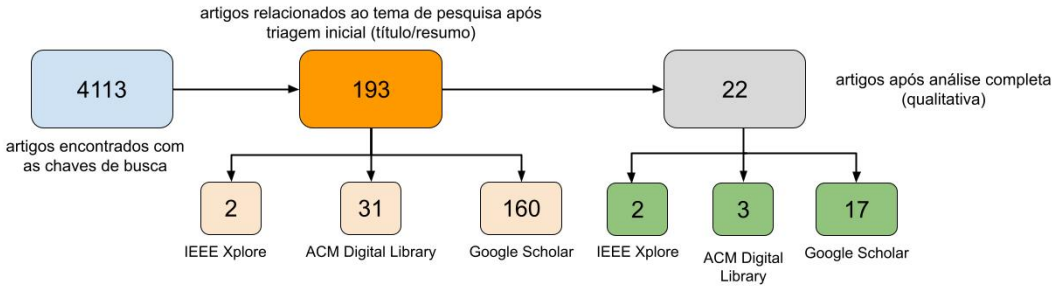

Figura 1. Fluxograma do trabalho de revisão bibliográfico.

A revisão sistemática de literatura foi utilizada para identificar as abordagens de prevenção contra a engenharia social, resultando na elaboração de uma tabela comparativa das principais soluções de segurança atualmente apresentadas pelas plataformas de *streaming*. Permitindo avaliar e destacar as principais diferenças em termos de acessibilidade e inovação no setor digital.

3.1. Engenharia Social

Em Bhattad e Patil (2023), afirma-se que atualmente as maiores ameaças cibernéticas são os ataques de engenharia social. Porém, o sucesso desses ataques são proveniente de tempos passados, em Wang, Zhu e Sun (2021) é mencionado que a engenharia social é famosa na comunidade *hacker* desde 1970. Ou seja, suas consequências vem de um longo período de tempo e cada vez mais seus métodos estão sendo aprimorados. Portanto, é importante a utilização de novas ferramentas, para reduzir as probabilidades de sucesso dos ataques. A Tabela 1, contém os métodos e suas vantagens contra a engenharia social.

Tabela 1. Métodos e Vantagens de Detecção e Prevenção de Ataques Cibernéticos Relacionados à Engenharia Social

Artigo	Método	Vantagens
Jamar et al. (2017)	Sistema de Detecção de Intrusão (IDS) e Sistema de Prevenção de Intrusão (IPS)	Monitoramento e análise contínua, redução de crimes cibernéticos
Heartfield e Loukas (2018)	*Cogni-Sense*	Alta taxa de detecção, capacita e incentiva os usuários a detectar e relatar ataques de engenharia social semântica
Nakamura e Dobashi (2019)	Detecção proativa	Antecipa domínios suspeitos e permite mitigação rápida
Li et al. (2021)	Abordagem *LIFE*	Integração de dados heterogêneos e detecção eficiente de fraudes
Khan (2023)	Criptografia robusta - Secure Socket Layer – Camada de Soquete Seguro (SSL) e Transport Layer Security – Segurança da Camada de Transporte (TLS)	Garante confidencialidade e integridade dos dados

3.2. Análise dos Métodos e das Vantagens na Prevenção de Ataques de Engenharia Social

Na pesquisa sobre o E-shield, por Jamar et al. (2017), mostrou a combinação entre um IPS e um IDS sendo eficaz na diminuição dos crimes virtuais, por meio de uma fiscalização e investigação das atividades exercidas no site. A aplicação do *Cogni-Sense* apresentada por Heartfield e Loukas (2018) mostrou ser eficiente na detecção de ataques de engenharia social semântica, com uma alta taxa, que confirma uma maior segurança para os sistemas do considerado o "elo mais fraco", que é o ser humano.

Nakamura e Dobashi (2019) apresentam a metodologia de Detecção proativa de sites de *phishing*, em que foi permitido antecipar domínios suspeitos, concedendo uma rápida diminuição dos casos, antes de ocorrer um dano significativo. Na abordagem *LIFE* utilizada em Li et al. (2021), revelou que a integração de dados heterogêneos em conjunto com uma rede neural de grafos, melhorou a detecção de fraudes. Por último, o Khan (2023) trouxe a utilização de duas formas de criptografia robustas para garantir uma maior integridade dos dados nos ambientes de realidade virtual imersivo.

3.3. Conclusão e Discussão sobre os Métodos

Os resultados mostram que as diferentes abordagens aplicadas foram eficazes no combate de ataques cibernéticos, seja através de sistemas de detecção e prevenção, ou pela antecipação de ameaças. Técnicas como a detecção proativa e redes neurais de grafos heterogêneos, reforçaram a importância da integração de dados para aumentar a segurança. O uso da criptografia em ambientes de *streaming* é uma solução robusta à medida que novas tecnologias surgem, como realidade aumentada. As pesquisas contribuíram para o avanço das técnicas de proteção cibernética, demonstrando a necessidade de abordagens contínuas e diversificadas para enfrentar as crescentes ameaças digitais.

3.4. Atuais Soluções Desenvolvidas pelas Plataformas de *Streaming* contra a Engenharia Social

A fim de apresentar as principais e atuais normas estipuladas pelas aplicações de transmissão *online*, foi realizada a construção da Tabela 2, tendo como base três principais exemplos de empresas de *streaming*: Netflix, Amazon Prime Video e Spotify. Foram avaliados aspectos de segurança como: proteção ao *login*, proteção contra ataques de engenharia social e defesa dos dados pessoais.

Tabela 2. Métodos propostos pelas plataformas de *streaming* contra ataques de engenharia social

Plataforma	Solução	Descrição
Netflix	Autenticação de dois fatores	Camada de proteção extra, que necessita de uma verificação, enviada ao e-mail ou celular do usuário na hora do login.
	Notificações	É transmitido ao usuário o monitoramento de novas atividades de login da sua conta.
	Proteção de dados	Recomendação de práticas para manter senhas e informações seguras.
	Orientação sobre *Phishing*	Orienta usuários a identificar possíveis tentativas de phishing, e como identificar mensagens suspeitas.
Amazon Prime Video	Proteção com PIN	É necessário um código PIN para acessar e fazer compras no perfil.
	Avisos de segurança	Alertas contra possíveis invasões, para deixar o usuário atento e conseguir proteger suas informações.
	Controle de conteúdo	Permite a configuração para restringir o acesso de materiais inadequados para crianças.
Spotify	Alertas	Monitoramento de possíveis invasões.
	Denúncia de E-mails	Oferece aos usuários um canal para envio de denúncias, onde é analisada e informada sua legitimidade.
	Proteção de Dados	Recomendação para utilizar senhas fortes e não compartilhar dados sensíveis.

Fonte: NETFLIX (2024), AMAZON (2024), SPOTIFY (2024)

As três utilizam uma proteção bem consistente de autenticação. O Spotify e a Netflix utilizam a autenticação de dois fatores, que garante uma etapa de verificação extra, proporcionando mais segurança. A Prime Video, oferece a utilização do PIN de segurança, que é necessário para acessar e fazer compras no aplicativo.

Foram apresentados diferentes métodos de proteção dos dados. A Prime Video faz o uso do controle parental, que permite restrigir o acesso de crianças, enquanto a Netflix e o Spotify utilizam a abordagem de recomendação, para manter senhas e informações

seguras, conscientizando as pessoas. As três também utilizam notificações para avisar os usuários de possivéis invasões.

Netflix e Spotify apresentam uma forma clara de fornecer orientações aos usuários sobre como reconhecer e relatar tentativas de *phishing*. A Netflix, por exemplo, fornece um canal de denúncia para as mensagens fraudulentas. Por outro lado, o Spotify oferece um meio para que os usuários denunciem o ataque via e-mail.

Apesar de todas demonstrarem ter uma boa solução para medidas de segurança, a Netflix se sobressai com uma metodologia de educar de forma consistente os usuários acerca dos ataques de *phishing*. Mostrando preocupação com seus usuários, o que é crucial para poder combater a vasta crescente das fraudes digitais. O Spotify também segue uma linha similar, incentivando a denúncia de e-mails de fraude eletrônica. Por outro lado, o Prime Video poderia utilizar um modo mais eficaz, promovendo campanhas sensibilizadoras acerca do ataque, se igualando com as práticas adotadas por outras plataformas.

4. Conclusão

O presente trabalho investigou as técnicas de engenharia social e como seus resultados afetam a segurança virtual dos recursos de *streaming*, apresentando como essas ameaças exploram o comportamento humano e afetam os sistemas. Embora as plataformas estudadas possuam tecnólogias avançadas, o fator humano ainda é um ponto vulnerável.

A partir da comparação das estratégias de segurança adotadas pelos aplicativos, verificou-se que soluções como autenticação multifator, campanhas educativas e monitoramento contínuo são eficazes, porém precisam ser constantemente aprimoradas e acompanhadas de maior investimento em capacitação do usuário.

O estudo reforça que a combinação de soluções tecnológicas robustas com iniciativas voltadas à conscientização do público é a abordagem mais eficaz para mitigar os impactos da engenharia social. Como proporcionar uma alfabetização digital entre os usuários. Esses procedimentos são extremamente importantes para contribuir com a resistência das comunidades online e preservar a integridade das plataformas digitais.

Portanto conclui-se, que a segurança cibernética em plataformas de *streaming* é um desafio dinâmico que exige respostas rápidas e flexíveis. A união entre empresas, pesquisadores e usuários é essencial para criar um ecossistema mais resiliente, onde a segurança digital e a experiência do usuário possam coexistir de maneira harmônica e eficiente. O trabalho também aponta para a necessidade de pesquisas futuras que explorem soluções inovadoras, como a aplicação de inteligência artificial e análise comportamental, para fortalecer ainda mais a proteção contra essas ameaças.

Referências

ADEWOLE, A; DUROSINMI, A; POLYETCHNIC, MA. Social engineering threats and applicable countermeasures. **African Journal of Computing & ICT**, Citeseer, v. 8, n. 2, 2015.

ALDAWOOD, Hussain; SKINNER, Geoffrey. An academic review of current industrial and commercial cyber security social engineering solutions. In: PROCEEDINGS of the 3rd International Conference on Cryptography, Security and Privacy. [S.l.: s.n.], 2019. P. 110–115.

AMAZON. **Amazon Prime Video Help**. Acesso em: 06 de outubro de 2024. 2024. Disponível em: https://www.primevideo.com/help.

BENAVIDES, Eduardo et al. Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. **Ciencia y Tecnología**, v. 13, n. 1, p. 97–104, 2020.

BHATTAD, Prasad; PATIL, Rakesh. Social Engineering in Cyber Security: A Comprehensive Review of Modern Threats, Challenges, and Counter Measures. Kesari Mahratta Trust, 2023.

GOMES, Vanessa; REIS, Joaquim; ALTURAS, Bráulio. Social Engineering and the Dangers of Phishing. In: 2020 15th Iberian Conference on Information Systems and Technologies (CISTI). [S.l.: s.n.], 2020. P. 1–7. DOI: 10.23919/CISTI49556.2020.9140445.

HEARTFIELD, Ryan; LOUKAS, George. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. **Computers & Security**, v. 76, p. 101–127, 2018. ISSN 0167-4048. DOI: 10.1016/j.cose.2018.02.020.

HIJJI, Mohammad; ALAM, Gulzar. A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. **IEEE Access**, v. 9, p. 7152–7169, 2021. DOI: 10.1109/ACCESS.2020.3048839.

JAMAR, Rishabh et al. E-shield: Detection and prevention of website attacks. In: IEEE. 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). [S.l.: s.n.], 2017. P. 706–710.

KHAN, Koffka. Security Challenges and Solutions in 360-Degree Augmented Reality Video Streaming: A Comprehensive Review, 2023.

KROMBHOLZ, Katharina et al. Advanced social engineering attacks. **Journal of Information Security and Applications**, v. 22, p. 113–122, 2015. Special Issue on Security of Information and Networks. ISSN 2214-2126. DOI: 10.1016/j.jisa.2014.09.005.

KUMAR, Anshul; CHAUDHARY, Mansi; KUMAR, Nagresh. Social engineering threats and awareness: a survey. **European Journal of Advances in Engineering and Technology**, Citeseer, v. 2, n. 11, p. 15–19, 2015.

LI, Zhao et al. Live-Streaming Fraud Detection: A Heterogeneous Graph Neural Network Approach. In: PROCEEDINGS of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining. Virtual Event, Singapore: Association for Computing Machinery, 2021. (KDD '21), p. 3670–3678. ISBN 9781450383325. DOI: 10.1145/3447548.3467065. Disponível em: https://doi.org/10.1145/3447548.3467065.

MALLICK, Md; NATH, Rishab. Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments, fev. 2024.

MOUTON, Francois; LEENEN, Louise; VENTER, H.S. Social engineering attack examples, templates and scenarios. **Computers & Security**, v. 59, p. 186–209, 2016. ISSN 0167-4048. DOI: https://doi.org/10.1016/j.cose.2016.03.004.

NAKAMURA, Akihito; DOBASHI, Fuma. Proactive Phishing Sites Detection. In: IEEE/WIC/ACM International Conference on Web Intelligence. Thessaloniki, Greece: Association for Computing Machinery, 2019. (WI '19), p. 443–448. ISBN 9781450369343. DOI: 10.1145/3350546.3352565. Disponível em: https://doi.org/10.1145/3350546.3352565.

NETFLIX. **Como manter sua conta segura**. Acesso em: 06 de outubro de 2024. 2024. Disponível em: https://help.netflix.com/en/node/13243.

NEUPANE, Ajaya et al. Do Social Disorders Facilitate Social Engineering? A Case Study of Autism and Phishing Attacks. In: PROCEEDINGS of the 34th Annual Computer Security Applications Conference. San Juan, PR, USA: Association for Computing Machinery, 2018. (ACSAC '18), p. 467–477. ISBN 9781450365697. DOI: 10.1145/3274694.3274730. Disponível em: https://doi.org/10.1145/3274694.3274730.

SPOTIFY. **Centro de ajuda do Spotify**. Acesso em: 06 de outubro de 2024. 2024. Disponível em: https://support.spotify.com/.

SUBRAYAN, S. et al. Multi-factor Authentication Scheme for Shadow Attacks in Social Network. In: 2017 International Conference on Technical Advancements in Computers and Communications (ICTACC). [S.l.: s.n.], 2017. P. 36–40. DOI: 10.1109/ICTACC.2017.19.

SUN, Nan et al. Data-Driven Cybersecurity Incident Prediction: A Survey. **IEEE Communications Surveys & Tutorials**, v. 21, n. 2, p. 1744–1772, 2019. DOI: 10.1109/COMST.2018.2885561.

SYAFITRI, Wenni et al. Social Engineering Attacks Prevention: A Systematic Literature Review. **IEEE Access**, v. 10, p. 39325–39343, 2022. DOI: 10.1109/ACCESS.2022.3162594.

VENKATESHA, Sushruth; REDDY, K Rahul; CHANDAVARKAR, BR. Social engineering attacks during the COVID-19 pandemic. **SN Computer Science**, Springer, v. 2, p. 1–9, 2021.

WANG, Zuoguang; ZHU, Hongsong; SUN, Limin. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. **IEEE Access**, v. 9, p. 11895–11910, 2021. DOI: 10.1109/ACCESS.2021.3051633.

WATSON, Hue et al. "We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. In: PROCEEDINGS of the 2020 CHI Conference on Human Factors in Computing Systems. Honolulu, HI, USA: Association for Computing Machinery, 2020. (CHI '20), p. 1–12. ISBN 9781450367080. DOI: 10.1145/3313831.3376605. Disponível em: https://doi.org/10.1145/3313831.3376605.