SISTEMA DE PROTEÇÃO ONLINE: OS USUÁRIOS ESTÃO SE SENTINDO PROTEGIDOS?

ONLINE PROTECTION SYSTEM: ARE USERS FEELING PROTECTED?

Gabriel Franco[1], Humberto Cáfaro Neto[2], Silvio C. Lopes[3]

[1]Faculdade de Tecnologia Professor José Camargo – Fatec Jales, humberto.cafaro@fatec.sp.gov.br
[2]Faculdade de Tecnologia Professor José Camargo – Fatec Jales, gabriel.franco01@fatec.sp.gov.br
[3]Faculdade de Tecnologia Professor José Camargo – Fatec Jales, silvio.lopes@fatec.sp.gov.br

Trabalho de Graduação apresentado à Faculdade de Tecnologia Prof. José Camargo - Fatec Jales, como requisito parcial para obtenção do título de Tecnólogo em Sistemas para Internet

RESUMO

O presente trabalho tem como objetivo avaliar a sensação dos usuários quanto a segurança dos dados oferecida pelos sistemas de proteção disponíveis online e recomendar algumas práticas de segurança e proteção dos dados. Para mesurar o parâmetro sensação de segurança foi conduzida uma pesquisa quantitativa para avaliar o nível de conscientização e adoção de medidas de proteção online pelos usuários. A pesquisa envolveu uma amostra representativa de usuários ativos na Internet e analisou suas atitudes e comportamentos em relação a segurança dos dados. Os resultados revelaram uma consciência em relação aos riscos associados à exposição de dados pessoais na internet e a utilização dela em ambientes diversos. Além disso, uma parcela significativa dos entrevistados compartilhava informações pessoais sensíveis na internet sem considerar as possíveis consequências. Com base nos estudos e dados coletados, concluiu-se que é essencial que as pessoas adotem medidas de proteção online para preservar a segurança de seus dados e manter-se atualizado sobre as melhores práticas de segurança e estar ciente dos riscos envolvidos na utilização e divulgação excessiva de informações pessoais na internet.

Palavras-chave: segurança da informação; proteção de dados; internet.

ABSTRACT

The present work aims to evaluate users' perception of data security provided by available online protection systems and recommend some data security and protection practices. In order to measure the parameter of security perception, a quantitative research was conducted to assess the level of awareness and adoption of online protection measures by users. The research involved a representative sample of active Internet users and analyzed their attitudes and behaviors regarding data security. The results revealed an awareness of the risks associated with the exposure of personal data on the internet and its use in various environments. Additionally, a significant portion of the respondents shared sensitive personal information on the internet without considering the potential consequences. Based on the studies and data collected, it was concluded that it is essential for individuals to adopt online protection measures to preserve the security of their data, stay updated on best security practices, and be aware of the risks involved in the excessive use and disclosure of personal information on the internet.

Keywords: information security; data protection; internet.

1 INTRODUÇÃO

O setor de Tecnologia da Informação (TI) se estabeleceu completamente e definitivamente em todos os segmentos. De acordo com o relatório de 2023 da *Global Overview Report* publicado pela Datareportal, atualmente, cerca de 64,4% da população mundial usa a Internet regularmente, representando mais de 5,16 bilhões de pessoas. A *Insider Intelligence*, publicou em 2021, um crescimento do comércio eletrônico com vendas globais próximas a atingir US$ 5 trilhões, com aumento de 27,6% em relação ao ano anterior, acreditando ter sido alavancada pela pandemia de Coronavírus (COVID-19).

Nos últimos anos, a quantidade de pessoas conectadas na Internet vem apresentando um crescimento exponencial, isto é, o cenário atual se mostra muito diferente se comparado a vinte anos atrás, onde sua utilização e popularidade ainda era pouco conhecida e explorada mundialmente, onde, até mesmo os profissionais mais ligados na área de tecnologia da informação e comunicação, desconheciam o poder dessa tecnologia. Desde então, a quantidade de dados e informações que circulavam nas redes aumentaram consideravelmente.

Com o advento da era digital, a internet tem se tornado uma ferramenta essencial para as empresas e usuários. No entanto, essa facilidade também atrai a atenção de indivíduos mal-intencionados, que buscam obter informações privadas e sensíveis através de programas maliciosos. Os chamados *crackers*, criam, otimizam e modificam softwares e hardwares para melhorar os sistemas de segurança e *hackers* burlam esses sistemas para obter vantagem ou causar danos e utilizam dessas brechas para os mais diversos fins lícitos ou ilícitos. Infelizmente, essa prática tem se tornado cada vez mais comum ao longo dos anos.

Com isso, empresas e usuários veem a necessidade de atualizações e investimentos na proteção de seus dados, aprimorando a segurança na utilização da rede por parte de usuários e colaboradores, na tentativa de neutralizar usuários, programas e ferramentas mal-intencionadas que continuam se adaptando, aprimorando suas formas de atentar contra usuários e empresas, de diversas formas. Para compreender a existência de tais ameaças, primeiro faz-se necessário entender como elas foram criadas e como funcionam.

Segundo Medeiros (2015), um dos pontos principais que cercam a segurança e proteção de dados é a criptografia, do grego *kryptós* (esconder) e *grápho* (escrita), que estuda formas de proteger dados a serem armazenados ou transmitidos de forma totalmente imune à perca ou roubo de informações, de maneira que apenas os proprietários tenham acesso aos dados. A criptografia é uma ciência antiga, que foi utilizada como metodologia para comunicação militar. Em meados de 1928, foi construída uma segunda versão dessa mesma máquina, a Enigma G, que visava melhorar a encriptação de sua antecessora manual, já que ela era mecânica e para decodificar a mensagem era necessário ter outra máquina que possuía a mesma "chave" que foi utilizada na sua encriptação. Após esse período, identificou-se ampla aplicação em atividades que exigiam uma maior segurança na troca de dados, como atividades bancárias, políticas e sociais. Seguindo essa necessidade e o surgimento dos computadores e seus sistemas, notou-se a grande janela de oportunidade de melhora desse recurso.

Com os avanços tecnológicos, a segurança da informação é um tema cada vez mais relevante e de grande importância. A facilidade na troca de informações também trouxe consigo um aumento nos vazamentos de dados, tornando-se uma preocupação constante para empresas e usuários. Devido a isso, é necessário acompanhar as mudanças e evoluções na área para garantir a proteção de informações sigilosas.

Os ataques cibernéticos são uma das maiores ameaças para a segurança da informação. Um exemplo recente disso é o "*WannaCry ransomware attack*", que ocorreu em 2017 e afetou cerca de 300.000 computadores em todo o mundo. Esse ataque utilizou uma vulnerabilidade no sistema operacional *Microsoft Windows*, conhecida como *EternalBlue*, que havia sido desenvolvida pela Agência de Segurança Nacional dos Estados Unidos (NSA) e vazada por

hackers em abril do mesmo ano. O objetivo do ataque era criptografar o conteúdo dos discos rígidos que executavam o sistema operacional *Microsoft Windows* e exigir pagamentos de resgate em *Bitcoin*. Segundo Souza (2014), o *Bitcoin* é uma moeda digital *peer-to-peer*, de código aberto, que não depende de uma autoridade central.

Diante dessa realidade, é essencial que empresas e usuários estejam preparados para lidar com possíveis ataques, por meio de medidas preventivas, como a implementação de sistemas de segurança eficazes e atualizados, além de investimentos em capacitação e treinamento de seus colaboradores.

O trabalho está organizado em cinco seções: a Seção 2 apresenta o referencial teórico, com a revisão de pesquisas e artigos que contextualizam o trabalho; a Seção 3 descreve a metodologia utilizada para a pesquisa e levantamento de informações; a Seção 4 apresenta de forma objetiva a análise da discussão dos resultados; e, por fim, a Seção 5 com as considerações finais e conclusão do trabalho.

2 REFERENCIAL TEÓRICO

Atualmente muitos sistemas passam por testes constantes cujo objetivo é localizar falhas ou brechas que comprometam a integridade dos dados que por eles são tratados. A seguir o artigo abordará sobre informações e dados, e algumas formas de proteção e suas falhas.

Ao que se refere a dados pode-se dizer que são pedaços de um quebra-cabeça que em sua forma única não possui relevância nenhuma, Segundo Elias (2022) “O dado não possui significado relevante e não conduz a nenhuma compreensão. Representa algo que não tem sentido a princípio”. Partindo disso pode-se dizer que o conjunto de dados seria considerado como informação, que por sua vez possui um valor inestimado e segundo Elias (2022) “A informação é a ordenação e organização dos dados de forma a transmitir significado e compreensão dentro de um determinado contexto”. A partir das informações pode-se chegar a tomadas de decisões e ainda a julgar pelo contexto das informações podem ser de suma importância para quem a detém.

2.1 DEFINIÇÃO DE SEGURANÇA

No contexto da segurança das informações, "segurança" pode ser descrita segundo Portal GTSI (2023) como um conjunto de medidas necessárias por garantir que a confidencialidade, integridade e disponibilidade das informações de uma organização ou indivíduo, de forma a preservar esta informação de acordo com necessidades específicas.

Segundo Barcelos (2019), a proteção da informação e as medidas de segurança, devem minimizar os riscos de perda de critérios como confidencialidade, integridade e disponibilidade. Os três pilares da Segurança da informação são:

- **Confidencialidade**: é a capacidade de um sistema permitir que somente usuários autorizados acessem determinada informação, ao mesmo tempo em que usuários não autorizados tentam acessá-la. A confidencialidade é considerada desejável para garantir a privacidade das informações que são tratadas e produzidas pelo software.
- **Integridade**: é a capacidade de um sistema impedir que uma informação seja alterada sem autorização ou, ao menos, detectar se isso ocorreu. É a qualidade do software que protege os dados ou informações contra modificações intencionais ou acidentais não autorizadas.
- **Disponibilidade**: a informação deve estar disponível quando ela for necessária. Manter a disponibilidade é importante para que usuários autorizados tenham acesso à informação correspondente sem que seja necessário esperar.

Um software confiável precisa ser íntegro e seguro tanto para eventos intencionais quanto para eventos não intencionais. Entende-se por eventos não intencionais os que podem ocorrer

quando um fator de ameaça não tem a intenção de causar dano, como, por exemplo, falhas na segurança no âmbito humano ou natural. Já os eventos intencionais ocorrem quando o fator de ameaça possui o objetivo de executar ataques que possam causar dano, e esses eventos, ocasionalmente, utilizam vulnerabilidades no software para comprometer a segurança como um todo.

2.2 PROTEÇÃO DE DADOS

Em 14 de agosto de 2018, foi criada a lei nº 13.709, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), que tem como objetivo proteger os direitos fundamentais da liberdade e privacidade, que engloba desde compras online a redes sociais e aplicativos de terceiros. Tal lei vem com uma forma de padronizar e criar regras para proteger os dados pessoais do usuário, aprovada pela Câmara dos Deputados e o Senado Federal desde 2018 e em vigor desde 2020, esta lei que também leva ao consentimento do usuário onde e de que forma seus dados estão sendo utilizados. É possível tratar dados sem consentimento se isso for indispensável para cumprir uma obrigação legal, executar política pública prevista em lei, realizar estudos via órgão de pesquisa, executar contratos, defender direitos em processo, preservar a vida e a integridade física de uma pessoa, tutelar ações feitas por profissionais das áreas da saúde ou sanitária, prevenir fraudes contra o titular, proteger o crédito, ou atender a um interesse legítimo, que não fira direitos fundamentais do cidadão (BRASIL, 2018).

2.3 CARACTERISTICAS NECESSÁRIAS PARA UM SOFTWARE SEGURO

De acordo com Kaspersky (2022), os pilares da segurança da informação, Confidencialidade, Integridade e Disponibilidade podem contar ainda com alguns mecanismos elaborados com o passar do tempo. São eles: controles físicos e lógicos, além de mecanismos de criptografia e assinatura digital, que são exemplificados no texto abaixo:

Controles físicos: são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta.

Controles lógicos: são barreiras que impedem ou limitam o acesso à informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal-intencionado. Existem mecanismos de segurança que apoiam os controles lógicos.

Mecanismos de criptografia: Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.

Assinatura digital: Um conjunto de dados criptografados, associados a um documento, o qual garante a integridade e autenticidade do documento associado, mas não a sua confidencialidade.

Em suma, um software ou sistema seguro devem garantir a proteção adequada dos dados e a minimização de riscos. Essas características incluem: robustez contra ataques cibernéticos, implementação de criptografia forte para proteger informações mais sensíveis, autenticação segura para verificar a identidade dos usuários, controle de acesso rigoroso para restringir acessos não autorizados, atualizações regulares de segurança para corrigir vulnerabilidades, monitoramento de atividades suspeitas, e auditorias para avaliar a conformidade com padrões de segurança. Esses elementos essenciais ajudam a garantir a integridade, confidencialidade e disponibilidade dos dados, proporcionando um ambiente confiável e protegido.

2.4 SENHAS, ROUBOS DE CONTAS E ERRO HUMANO

Uma pesquisa realizada pela empresa de segurança cibernética Trend Micro (2022) revelou que 71% dos funcionários de empresas nos Estados Unidos já sofreram um incidente de segurança cibernética enquanto trabalhavam remotamente. A pesquisa também mostrou que 84% dos líderes de TI acreditam que os trabalhadores remotos representam um risco maior para a segurança cibernética do que os funcionários no local de trabalho. Um estudo da USENIX (WASH et al., 2016) sobre o uso de senhas relata:

> Realizamos um estudo que combina respostas de pesquisas de autorrelato com medidas de comportamento online real coletadas de 134 participantes ao longo de seis semanas. Descobrimos que as pessoas tendem a reutilizar cada senha em 1,7 a 3,4 sites diferentes, reutilizam senhas mais complexas e, principalmente, tendem a reutilizar senhas que precisam ser digitadas com frequência.

Estas duas pesquisas mostram fatos interessantes e conectados, onde vários usuários e trabalhadores se mostram inseguros em seus locais de trabalho e estudo.

Recentemente de acordo com uma pesquisa da universidade Stony Brook (LI; YEPURI; NIKIFORAKIS, 2023), várias contas do *YouTube* vêm sendo afetadas por grupos maliciosos tentando criar fraudes relacionadas com criptomoeda, usando arquivos e sites disfarçados de outros e roubando informações por pequenas brechas do site da *Google*. Isso vem aumentando e piorando. Um exemplo relevante é o caso do youtuber Linus Tech Tips, que atua na área de tecnologia da informação. Em seu vídeo intitulado *"My channel was deleted last night*" (Meu canal foi deletado na noite passada), ele relata que sua conta foi invadida e todos os seus vídeos foram deletados por um *hacker* que substituiu seus vídeos por transmissões ao vivo de golpes de criptografia. Agindo rapidamente e contatando o *YouTube,* Linus Tech Tips conseguiu salvar seu canal, que teria desaparecido caso ele não tivesse tomado medidas imediatas. O ataque só foi possível porque um de seus funcionários clicou em um *link* de uma oferta de patrocínio, que continha um programa malicioso capaz de roubar senhas e dados armazenados no navegador. Esse episódio destaca que, mesmo com as melhorias na segurança online, até mesmo uma empresa como o *Google* pode ser vítima de um dos maiores perigos no mundo digital: o erro humano.

Considerando o exposto, é possível afirmar que, apesar de todas as proteções e defesas existentes, uma das maiores fraquezas de todas as empresas ainda é o erro humano. Segundo Pollock (2017), da Universidade de Kennesaw,

> O erro humano é um problema de segurança complexo e difícil de definir, que tem desafiado a criação de um esquema de classificação estruturado e padronizado. Embora o erro humano possa nunca ser completamente eliminado das tarefas que as pessoas desempenham devido à falta de consciência situacional ou à falta de treinamento adequado, o primeiro passo para fazer melhorias em relação ao status é estabelecer um esquema unificado para classificar tais erros de segurança.

Estes erros humanos acontecem de vários modos sendo a Engenharia Social a principal via de indução. A engenharia social é uma técnica utilizada por *hackers* e *crackers* para manipular e explorar a psicologia humana com o objetivo de obter informações confidenciais, acesso não autorizado a sistemas ou persuadir as pessoas a realizar ações que beneficiem o atacante. É uma forma de ataque que se baseia na interação e manipulação das pessoas, em vez de explorar apenas vulnerabilidades técnicas.

O *National Institute of Standards and Technology* (NIST, 2017) dos Estados Unidos define a engenharia social como "a prática de obter acesso não autorizado, divulgar informações confidenciais ou induzir as pessoas a realizar ações prejudiciais, geralmente por meio de

manipulação psicológica e exploração da confiança". A engenharia social pode envolver diferentes táticas, como:

Phishing: É uma técnica em que os atacantes se passam por entidades confiáveis, como bancos, empresas ou serviços online, e enviam mensagens falsas para obter informações confidenciais, como senhas, números de cartão de crédito ou informações pessoais. Essas mensagens podem ser enviadas por e-mail, mensagens de texto, redes sociais ou outras formas de comunicação eletrônica.

Pretexting: Envolve a criação de uma narrativa fictícia ou uma desculpa para obter informações de uma pessoa. O atacante pode se passar por uma pessoa confiável, como um representante de suporte técnico, um colega de trabalho ou um funcionário de uma empresa, e solicitar informações sensíveis ou acesso a sistemas.

Quid pro quo: Nessa técnica, o atacante oferece algo de valor em troca de informações sensíveis. Por exemplo, eles podem se passar por um pesquisador de mercado e oferecer um brinde ou recompensa em troca de informações pessoais ou acesso a um sistema.

Tailgating: Envolve aproveitar a confiança das pessoas em um ambiente físico. O atacante segue ou entra em um local restrito juntamente com uma pessoa autorizada, explorando a cortesia ou falta de atenção para obter acesso não autorizado.

Essas são apenas algumas das táticas comuns de engenharia social, e os ataques podem ser adaptados e combinados de várias maneiras para aumentar as chances de sucesso. É importante estar ciente da engenharia social e adotar medidas de proteção, como a conscientização sobre ameaças, a verificação de identidade, a implementação de políticas de segurança cibernética para mitigar os riscos associados a esse tipo de ataque.

3 METODOLOGIA

Visando atingir os objetivos deste artigo, foram realizadas pesquisas bibliográficas com o objetivo de entender os principais conceitos relativos à segurança, proteção de dados e segurança em softwares e sistemas de informação e analisar a conscientização e adoção de medidas de proteção online por parte dos usuários da internet. Fontes acadêmicas, artigos científicos, livros, documentos técnicos e publicações relevantes foram consultados para embasar teoricamente o estudo.

Com base nos conhecimentos adquiridos na pesquisa bibliográfica, foi elaborado um questionário utilizando a plataforma *Google Forms*. O questionário abordou temas relacionados à conscientização sobre segurança cibernética, comportamentos e práticas de proteção de dados dos usuários da internet. Questões relacionadas ao compartilhamento de informações pessoais, conhecimento sobre ameaças online e sobre a sensação de segurança ao utilizar os diversos serviços oferecidos pela rede mundial de computadores, também foram utilizadas.

A amostra foi composta por 95 participantes alunos de cursos de tecnologias da informação e usuários assíduos da internet. Os participantes foram convidados a responder o questionário online por meio do link fornecido.

Após a coleta dos dados, foram realizadas análises e tabulação dos dados para avaliar as respostas e identificar tendências e padrões relacionados à proteção de dados e segurança em softwares e sistemas de informação, como explicitados na seção a seguir.

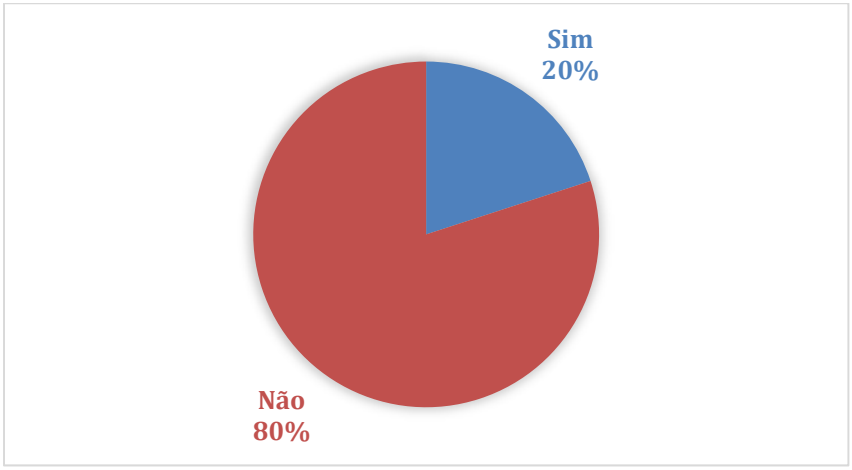
4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Para o presente trabalho, optou-se por realizar uma pesquisa quantitativa, que é amplamente utilizada para garantir a precisão dos resultados em análises estatísticas. Esse tipo de pesquisa permite obter quantitativos específicos para cada resposta, ao contrário da pesquisa

qualitativa, na qual as respostas são mais abertas e variáveis. Com a pesquisa quantitativa, buscou-se obter dados mais precisos e confiáveis para embasar as análises.

A seguinte pesquisa a foi enviada para discentes de cursos de Tecnologia da Informação da Faculdade de Tecnologia de Jales (Fatec), onde um total de 95 pessoas responderam as questões, todas elas relacionadas com segurança online de usuários, e opiniões sobre tópicos que vão desde a segurança de suas contas e senhas, a segurança em áreas de trabalho e estudo.

Gráfico 1 – Você acredita que seus dados e senhas estão seguros quando armazenados em navegadores como Google Chrome e Mozilla Firefox?

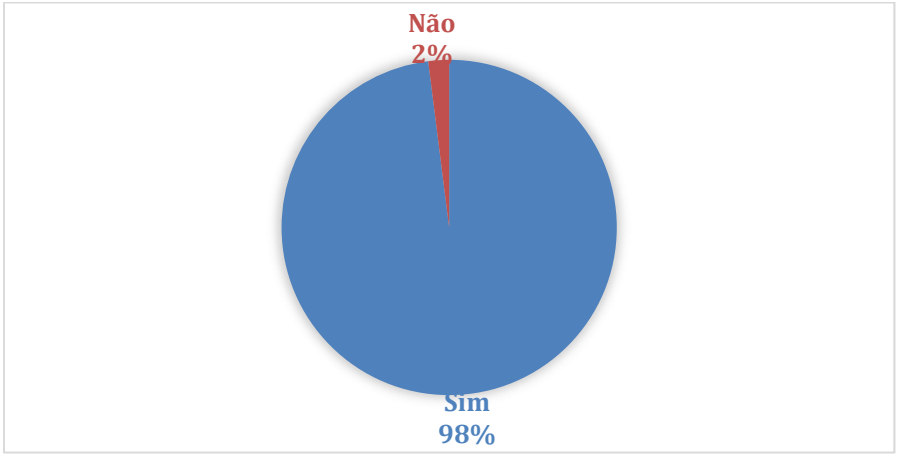


Fonte: Elaborado pelos autores

No Gráfico 1, acima, observou-se que 80% dos usuários não se sentem seguros armazenando seus dados e senhas em navegadores, enquanto apenas 20% afirmaram confiar nessas ferramentas para guardar suas informações pessoais. Isso indica que muitos usuários não confiam plenamente nesses aplicativos, mesmo que eles facilitem o uso de suas contas online.

De acordo com a facilidade de acesso a dados e informações pessoais por meio de navegadores, é comum que usuários enfrentem riscos significativos de roubo de informações caso sejam descuidados. Nesse contexto, é recomendável que tais informações sejam armazenadas exclusivamente em computadores pessoais, a fim de evitar acidentes ou uso indevido desses dados.

Gráfico 2 – Já percebeu que quando você pesquisa um assunto específico nos sites de buscas, tais tópicos começaram a serem recomendados em sites como Facebook, Youtube?

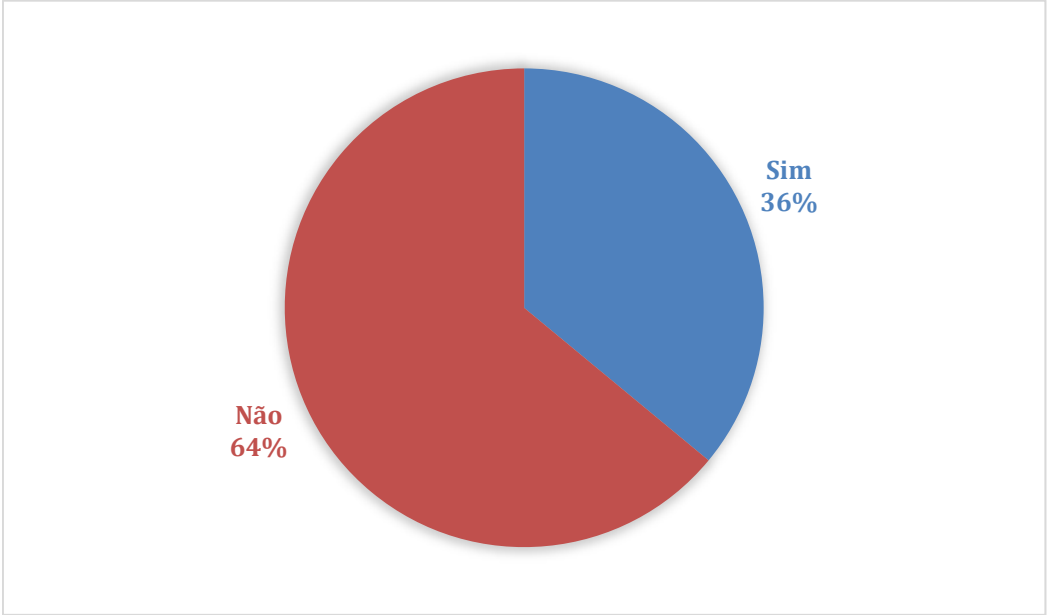


Fonte: Elaborado pelos autores

Neste Gráfico 2, apenas 2% dos usuários não perceberam que as mídias sociais utilizam informações de suas pesquisas e interesses para aprimorar a busca por conteúdo dentro da plataforma. Esse é um recurso comum nessas plataformas, que visa facilitar a busca por conteúdo de interesse dos usuários.

Caso o usuário não queira que suas pesquisas e interesses sejam registrados por esses sites, a melhor abordagem seria utilizá-los sem efetuar o *login* em sua conta, uma vez que as recomendações são baseadas no que o usuário está visualizando no momento. Dessa forma, se o usuário deseja evitar que um tópico pesquisado uma única vez polua sua página, é recomendado que realize a pesquisa em uma aba anônima do navegador e não efetuar *login* em sua conta.

Gráfico 3 – Você acredita valer a pena ter informações pessoais disponíveis para grandes companhias para melhorar a sua experiência na internet?

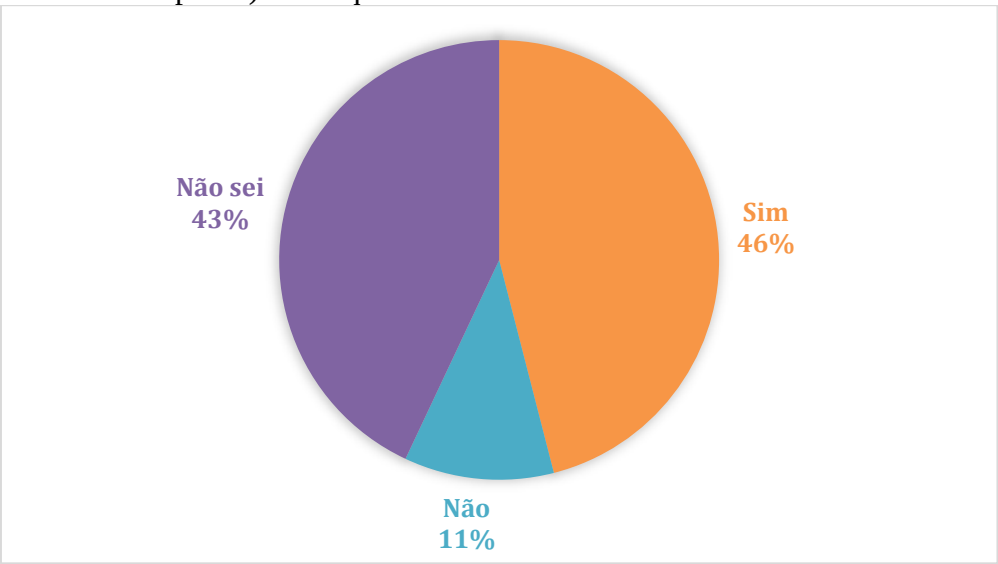


Fonte: Elaborado pelos autores

No Gráfico 3 pode-se observar que 64% dos usuários não consideram que o compartilhamento de suas informações pessoais com grandes empresas valha a pena, possivelmente devido a preocupações pessoais ou outras razões. Enquanto os outros 36% acreditam que compartilhar essas informações pode facilitar o uso dos sites dessas grandes empresas e melhorar a experiência do usuário, especialmente ao procurar informações sobre produtos específicos ou temas desconhecidos. Esses resultados mostram que, embora muitos usuários estejam dispostos a compartilhar suas informações, ainda há uma falta de confiança em relação às grandes empresas ao uso de seus dados pessoais.

Considerando o uso dessas informações pelas grandes companhias, na falta de confiança, são necessárias algumas providências como: Ler e entender políticas de privacidade; controlar as configurações de privacidade, optando por serviços com foco na privacidade; evitar fornecer informações desnecessárias, estar sempre atento a *cookies* e rastreamento; ser seletivo ao compartilhar em redes sociais e manter-se informado.

Gráfico 4 – O lugar onde você trabalha ou estuda utiliza-se de proteção contra vírus, DDOS (DDOS ou negação de serviço distribuída, é um tipo de ataque cibernético que tenta indisponibilizar um website ou recurso de rede inundando-o com tráfego mal-intencionado e deixando-o incapaz de operar.) ou ataques *hackers*?

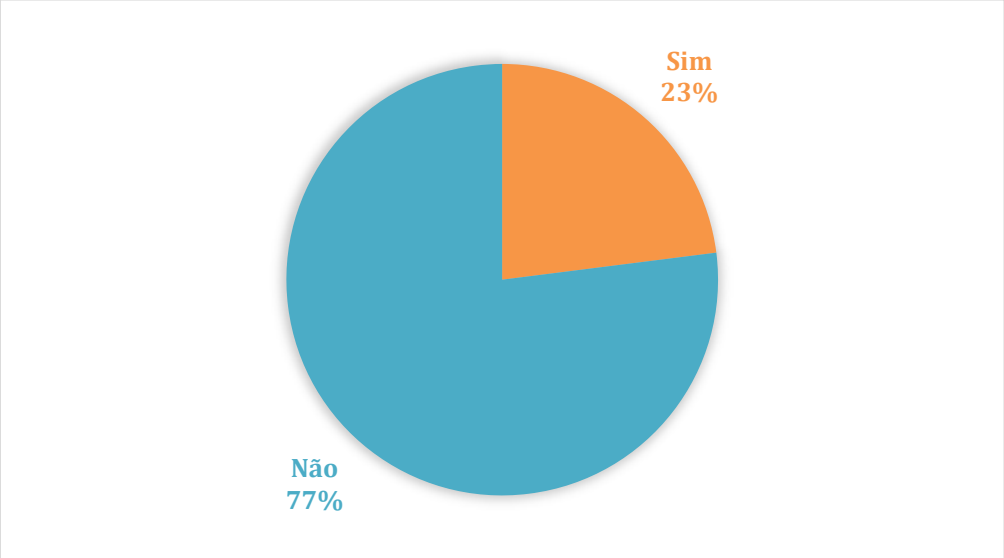


Fonte: Elaborado pelos autores

Segundo o Gráfico 4, 43% dos entrevistados desconhecem se seus locais de estudo ou trabalho possuem medidas de proteção adequadas contra ataques *hackers*, vírus e DDOS, o que pode ser preocupante, considerando a possibilidade de um ataque ocorrer acidentalmente através de um usuário que abra um programa malicioso de forma não intencional. Com 46%, os entrevistados afirmaram que seus locais de estudo e trabalho possuem proteção adequada, enquanto 11% afirmaram que não possuem proteção em seus respectivos locais.

Existem várias maneiras de verificar a segurança de uma empresa ou escola frequentada pelos usuários. Alguns exemplos incluem a verificação da implementação de sistemas de prevenção de intrusões (IPS) e detecção de intrusões (IDS). Além disso, pode-se investigar se a organização passou por auditorias de segurança ou obteve certificações relevantes, como a certificação ISO 27001, um padrão internacional de segurança da informação que estabelece diretrizes e requisitos para a implementação de um sistema de gestão de segurança da informação eficaz. Através dessas e outras abordagens, é possível avaliar o nível de segurança de uma empresa

Gráfico 5 – Os EULA (Contrato de Licença de Usuário Final) costumam conter informações sobre o uso de seus dados. Você já leu algum por completo?

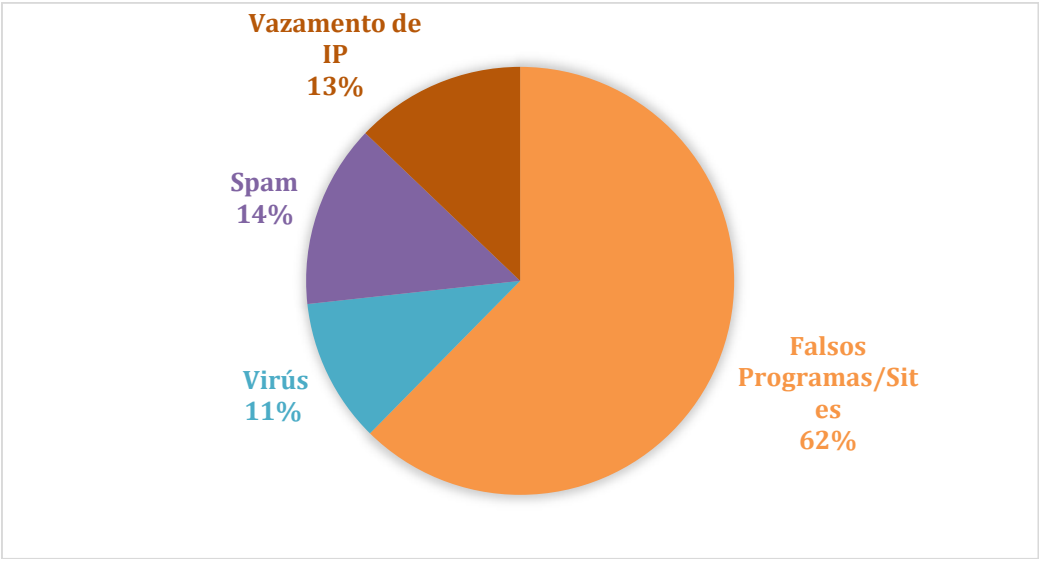


Fonte: Elaborado pelos autores

No Gráfico 5 é mostrado que a grande maioria dos usuários, representando 77% das respostas, simplesmente ignora o EULA. Porém, chama atenção o fato de que 23% dos usuários afirmaram ler esses termos antes de aceitá-los. Esses resultados ressaltam a importância de se apresentar esses contratos de maneira clara e acessível ao público, a fim de garantir que os usuários possam entender e consentir com as políticas de uso dos serviços.

É importante que os usuários leiam os termos de uso e políticas de privacidade das empresas, pois podem conter informações relevantes sobre as medidas de proteção de informações, a abordagem de privacidade adotada, e as responsabilidades individuais no uso seguro do software ou serviço. A identificação de possíveis brechas nessas políticas pode representar um risco significativo para a empresa ou usuário.

Gráfico 6 – Das opções abaixo qual delas você considera ser a forma mais comum de *hackear*?

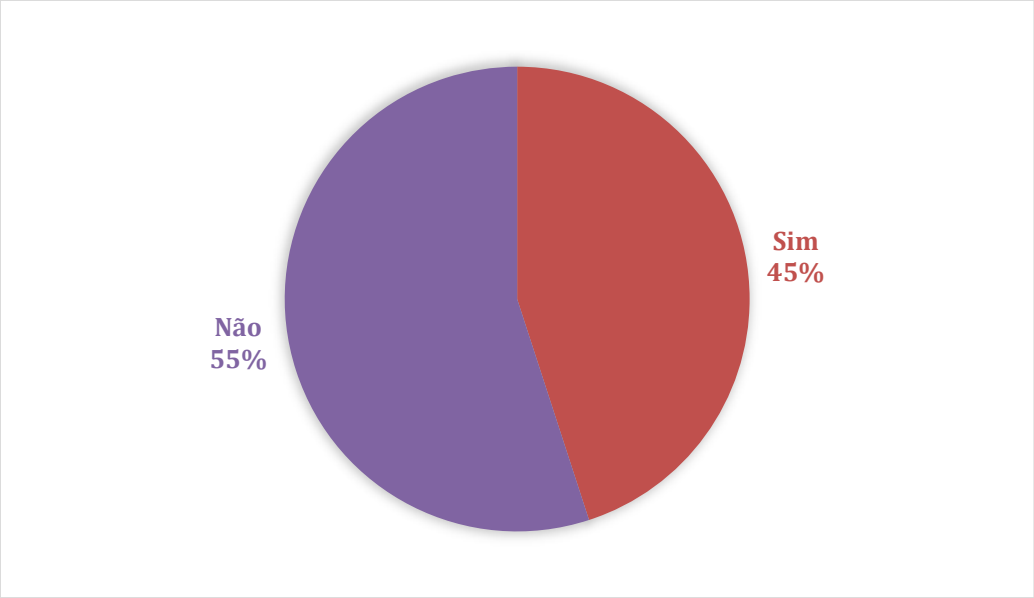


Fonte: Elaborado pelos autores

Neste Gráfico 6, nota-se algumas respostas interessantes. Apesar de atualmente a maioria dos aplicativos e programas terem melhores defesas contra vírus, diferentemente do que foi no passado, 11% dos usuários ainda se preocupam com o perigo que eles representam. Além disso, 14% dos usuários acreditam que *spams* ainda são perigosos, embora eles sejam filtrados na maioria das vezes e raramente são vistos por usuários comuns. Outra preocupação mencionada por 13% das respostas é o vazamento de endereço IP, embora esse tipo de ameaça também seja raro devido às melhorias na segurança *online*. No entanto, a resposta mais comum, com 62% das respostas, é a preocupação com o roubo de dados por meio de sites e programas falsos, que se passam por oficiais e enganam seus usuários.

Existem diversas formas pelas quais os usuários podem se proteger contra ataques *hackers*. Uma das principais medidas preventivas é o cuidado com a engenharia social, como o *phishing*, por exemplo. *Links* e e-mails suspeitos representam grandes perigos quando se trata desses *hackers*. O usuário deve sempre suspeitar de qualquer *link* estranho ou suspeito e manter seus softwares atualizados para corrigir eventuais vulnerabilidades.

Gráfico 7 – Você acredita estar seguro quando utiliza a rede do seu ambiente de trabalho ou faculdade?

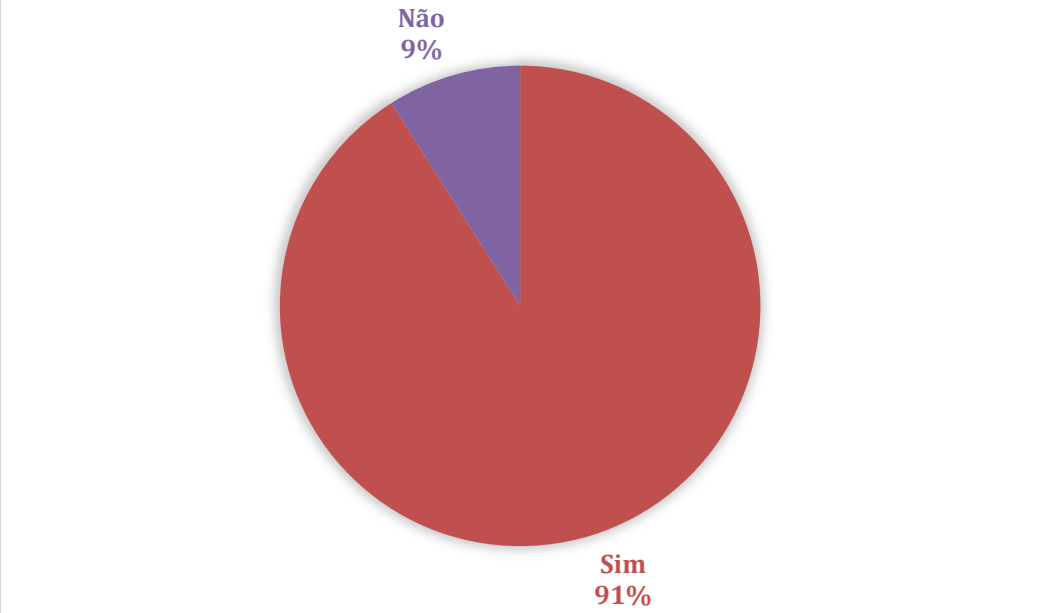


Fonte: Elaborado pelos autores

No Gráfico 7 é possível observar os seguintes resultados: Dos entrevistados, 45% afirmaram sentir-se seguros em seus locais de trabalho e estudo, o que pode indicar uma confiança nas medidas de segurança adotadas pelas instituições em que atuam ou frequentam. Por outro lado, 55% das respostas revelaram uma sensação de insegurança nesses mesmos ambientes, o que pode estar relacionado a uma percepção de vulnerabilidade em relação a possíveis ataques cibernéticos ou violação de dados pessoais.

Ao utilizar seus dados em plataformas *online*, o usuário deve ter sempre em mente que está em um ambiente público e, portanto, deve tomar precauções em relação às suas senhas e informações pessoais. Conforme destacado na descrição do Gráfico 1, é essencial nunca salvar dados em aplicativos ou computadores fornecidos por empresas, a fim de evitar erros de segurança.

Gráfico 8 – Você acha que sua empresa ou faculdade precisa de investimentos em segurança de dados?



Fonte: Elaborado pelos autores

No último, Gráfico 8, pode-se observar um resultado expressivo, onde 91% dos usuários concordam que seus locais de trabalho e estudo devem investir em segurança, o que demonstra uma preocupação crescente em relação à proteção dos dados. Por outro lado, apenas 9% dos respondentes discordam dessa necessidade e acreditam que não é essencial investir em medidas de segurança, reforçando a importância de se investir na conscientização e/ou em treinamentos específicos dos usuários quanto ao uso da tecnologia e das redes, visando garantir a integridade e a confidencialidade dos dados em ambientes corporativos ou educacionais.

Com base nos resultados obtidos, é evidente que um aumento nos investimentos em segurança de dados pode ser extremamente valioso para os usuários ou trabalhadores em seus locais de estudo e trabalho. Essa medida não apenas tranquiliza as pessoas, mas também proporciona maior facilidade em suas tarefas, reduzindo a sensação de insegurança ao lidar com informações confidenciais.

5 CONSIDERAÇÕES FINAIS

O presente artigo abordou questões como segurança nas redes e internet, bem como os diversos sistemas de proteção online, e o sentimento dos usuários quanto a utilização das redes, ressaltando a importância de medidas de proteção que visam garantir a segurança das informações nestes ambientes. O resultado da pesquisa apresentada na análise e discussão dos resultados, mostraram a importância da conscientização e a apropriação de práticas seguras por parte das organizações e usuários.

A segurança das redes e da internet tem apresentado melhorias em seu potencial a cada ano, principalmente no que se refere ao reconhecimento de elementos maliciosos e o bloqueio destes por intermédio de programas de defesa. Contudo, mesmo com a utilização de tais programas, usuários mal-intencionados ou a sofisticação das ameaças, ainda encontram pequenas brechas, sendo uma das maiores delas a falta de conhecimento dos usuários em relação à proteção online.

Os usuários de redes, mesmo aqueles que trabalham ou estudam na área de tecnologia da informação, como mostrado na pesquisa, expressam sentimento de insegurança em relação à proteção de seus dados, mesmo possuindo um conhecimento na área. Isso pode ser atribuído a

diversos fatores, tais como: falta de interesse em analisar os termos de uso e licenças de software (EULAs), desconhecimento sobre a segurança de seus ambientes de trabalho ou estudo, a não utilização de programas específicos e treinamentos, a não utilização de *firewalls* ou programas antivírus. Essa constatação evidencia que tais medidas sejam fundamentais para proteger dados pessoais e informações sensíveis de acessos não autorizados e ataques maliciosos.

É evidente que a utilização de programas voltados para a segurança das informações na rede e na internet não apenas protege os dados pessoais dos usuários e organizações, mas também contribui para a manutenção da integridade e disponibilidade dos dados, prevenindo perdas financeiras e danos à reputação de usuários e organizações.

Diante desse cenário, torna-se imprescindível que as empresas invistam e aprimorem seus recursos de proteção de dados, incluindo o aperfeiçoamento de sistemas de criptografia, mecanismos de proteção, bem como a constante verificação e atualização de seus sistemas. Além disso, a conscientização dos usuários sobre aspectos como a engenharia social é crucial para eliminar ou reduzir erros humanos que podem comprometer a segurança dos dados. Mesmo com toda a evolução tecnológica, usuários mal-intencionados como os *hackers* e *crackers* também estão aprimorando suas técnicas para enfrentar novas situações, o que torna a segurança das redes e internet uma corrida longa e contínua para todos, por fim, ressalta-se ainda que a segurança das redes não é só uma responsabilidade dos usuários, mas também das empresas e órgãos reguladores, e a cooperação entre as partes é crucial para a promoção de um ambiente virtual mais seguro.

REFERÊNCIAS

BARCELOS, N. **Os pilares da segurança da informação**: quais são e qual sua importância para uma segurança efetiva. 2019. Disponível em: https://tripla.com.br/os-pilares-da-seguranca-da-informacao/. Acesso em: 20 abr. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 2 maio 2022.

ELIAS, D. **Dados vs informação**: qual a diferença? Disponível em: https://www.binapratica.com.br/dados-x-informacao. Acesso em: 2 maio 2022.

KASPERSKY. **O que é criptografia de dados?**: definição e explicação. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/encryption. Acesso em: 20 abr. 2022.

LI, X.; YEPURI, A.; NIKIFORAKIS, N. Double and nothing: understanding and detecting cryptocurrency giveaway scams. **Network and Distributed System Security**. San Diego, 2023. Disponível em: https://www.securitee.org/files/cryptoscams_ndss2023.pdf. Acesso em: 2 maio 2023.

MEDEIROS, F. **Uma breve história da criptografia**. 2015. Disponível em: https://cryptoid.com.br/banco-de-noticias/a-historia-da-criptografia/. Acesso em: 23 maio 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. **Computer Security Incident Handling Guide**. 2017. Disponível em: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf. Acesso em: 8 jun. 2023.

POLLOCK, T. Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS). **KSU Proceedings on Cybersecurity Education**: research and practice, n. 2, 2017. Disponível em: https://digitalcommons.kennesaw.edu/ccerp/2017/research/2/. Acesso em: 15 abr. 2023.

PORTAL GTSI. **O que é segurança da informação?** 2023. Disponível em: https://www.portalgsti.com.br/seguranca-da-informacao/sobre/. Acesso em: 8 jun. 2023.

SOUZA, M. W. F. **Bitcoin**: uma análise jurídica dessa moeda virtual. 2014. Disponível em: https://www.jusbrasil.com.br/artigos/bitcoin-uma-analise-juridica-dessa-moeda-virtual/147062295. Acesso em: 2 maio 2023.

TREND MICRO. **Navigating New Frontiers**. 2022. Disponível em: https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf. Acesso em: 10 abr. 2023.

WASH, R. *et al*. Understanding password choices: how frequently entered passwords are re-used across websites. *In*: SYMPOSIUM ON USABLE PRIVACY AND SECURITY, 12th., Denver, 2016. **Proceedings** [...]. Denver: Usenix, 2016. Disponível em: https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-wash.pdf. Acesso em: 2 maio 2023.