Segurança da Informação em Dispositivos Móveis: Perspectivas e Comportamento dos Usuários

Antonio Machado*, Marcos Santos*, Iara Porfirio†, Carlos Volpi††, Éder Gualberto††
*Instituto Federal de Sergipe, Aracaju, Brasil
† Universidade Federal de Alagoas, Maceió, Brasil
†† Universidade de Brasília, Distrito Federal, Brasil.
E-mail: antonio.machado@ifs.edu.br, marcos.pereira@ifs.edu.br, iara.angelino95@gmail.com, cvolpi@ifes.edu.br, edergual@gmail.com

***Abstract*—The advancement of technology has significantly increased the use of smartphones and tablets, with many people using these devices to store data, send messages, browse the internet, and perform other tasks. Consequently, the theft of personal data has become more common, aiming to store and use personal information such as passwords, bank details, photos, and videos illegally. This paper aims to identify whether mobile device users follow good security practices. The results reveal the main areas where users fail to adequately protect themselves and highlight the lack of knowledge about security standards.**

***Keywords*—SIEM; Threat Detection; Information Security.**

***Resumo*—O avanço da tecnologia aumentou significativamente o uso de smartphones e tablets, com muitas pessoas utilizando esses dispositivos para armazenar dados, enviar mensagens, navegar na internet e realizar outras tarefas. Consequentemente, o roubo de dados pessoais tornou-se mais comum, com o objetivo de armazenar e usar informações pessoais, como senhas, dados bancários, fotos e vídeos, de maneira ilegal. Este trabalho tem como objetivo identificar se os usuários de dispositivos móveis seguem boas práticas de segurança. Os resultados revelam os principais pontos em que os usuários falham em se proteger adequadamente e evidenciam a falta de conhecimento sobre normas de segurança.**

***Palavras-chave*—SIEM, Detecção de ameaças, Segurança da informação.**

I. Introdução

No cenário atual, o uso de dispositivos móveis, como smartphones e tablets, está crescendo exponencialmente, com usuários utilizando a internet para redes sociais, jogos, mensagens instantâneas, compras online e diversas outras atividades [2]. No entanto, esse aumento de uso também traz riscos, como o acesso não autorizado por pessoas mal-intencionadas, resultando em roubo de dados e uso indevido dessas informações [1]. Muitas vezes, o vazamento de dados ocorre porque os usuários não utilizam recursos tecnológicos adequados, como antivírus, senhas fortes, sistemas operacionais atualizados e outros mecanismos de segurança [5].

A segurança cibernética para dispositivos móveis é uma questão cada vez mais relevante na era digital. Com o rápido desenvolvimento da tecnologia móvel e a massificação de smartphones e tablets, esses dispositivos se tornaram alvos preferenciais para hackers e criminosos cibernéticos. A falta de conscientização e a adoção insuficiente de medidas de segurança podem expor os usuários a riscos significativos, como o roubo de dados pessoais, a violação de privacidade, infecção por malware e o acesso não autorizado a informações sensíveis [3].

Proteger dispositivos móveis envolve a implementação de um conjunto de práticas e medidas destinadas a garantir a segurança tanto do equipamento quanto dos dados nele armazenados e transmitidos. Há várias áreas cruciais a serem consideradas ao tratar da segurança cibernética para dispositivos móveis. Em primeiro lugar, é imprescindível proteger o dispositivo com senhas fortes ou mecanismos de autenticação biométrica, como reconhecimento facial ou impressão digital. Essas medidas ajudam a evitar acessos não autorizados, especialmente em casos de perda ou roubo do aparelho [9].

Um estudo realizado pela Surfshark mostrou que o Brasil é o sexto país mais atingido por vazamento de informações em 2021 [12]. Entre os meses de janeiro e novembro, 24,2 milhões de usuários tiveram suas informações vazadas na internet a partir de ataques ou brechas em sistemas. A pesquisa ainda informa que os Estados Unidos lideram a lista de incidentes com 212,4 milhões de contas atingidas e um crescimento de 22% em relação ao ano 2020. Já o Irã ocupa o segundo lugar, com um aumento de 10.84% em 2021 quando comparado com o volume de vazamentos registrado no período anterior [12].

Apesar do crescente número de ataques, os celulares ainda não recebem a devida atenção em relação a sua segurança por parte de seus usuários [10]. É notória a diferença dos cuidados com a segurança dos celulares em comparação com os computadores pessoais. Portanto, empregar recursos, ferramentas

e boas práticas que visam a proteção dos celulares e de seus dados são essenciais para a redução da probabilidade desses equipamentos se tornarem alvos de ataques, impedindo assim que informações sejam acessadas indevidamente [4].

Embora exista um número considerável de pesquisas voltadas para a segurança em celulares, evidências sugerem que são poucas as contribuições que determinam quais boas práticas de segurança devem ser adotadas pelos usuários que objetivam proteger seus dados. Além disso, aspectos psicológicos e comportamentais do usuário também contribuem para que a proteção nos ambientes móveis se torne ainda mais desafiadora.

Visando a segurança da informação em dispositivos móveis, o objetivo deste trabalho foi observar como os usuários estão protegendo seus aparelhos celulares contra ataques a roubo de dados, verificando assim, quais os níveis e medidas de proteção foram adotados e os tipos de recursos de segurança da informação que são utilizados, além de compreender se os indivíduos utilizam boas práticas que são recomendadas pelos profissionais da segurança da informação.

II. Metodologia

A. Planejamento do Estudo

A pesquisa foi baseada em um levantamento bibliográfico e na aplicação de um formulário eletrônico adaptado de Xxxxxx et al. (XXXX), criado na plataforma Google Forms. O formulário incluiu o Termo de Consentimento Livre e Esclarecido (TCLE), explicando os detalhes da pesquisa e a finalidade dos dados coletados. O formulário foi distribuído amplamente, visando atingir um público diversificado, incluindo alunos, professores e técnicos administrativos da instituição, além de um público externo. Foi disponibilizado por e-mail e mensagens via WhatsApp durante um período de seis dias.

B. Artefato

O formulário utilizado para obtenção dos dados possuía ao todo 23 (vinte e três) perguntas objetivas, permitindo que os participantes selecionassem mais de uma alternativa em algumas respostas. As perguntas abordavam temas como uso de senhas e métodos de bloqueio, fontes de download de aplicativos, utilização de antivírus, atualização dos sistemas operacionais, utilização de redes sem fio, armazenamento e compartilhamento de senhas, utilização de serviços de computação em nuvem e backup de dados, além de segurança física dos dispositivos móveis.

Para coletar opiniões dos participantes sobre situações não contempladas no formulário, ou para qualquer observação sobre a pesquisa, os participantes poderiam incluir comentários ao final do formulário.

Após a coleta de dados, as informações foram processadas para apresentar os níveis de preferência bancária e compreender como as pessoas utilizam as ferramentas tecnológicas digitais dos bancos.

III. Análise dos Resultados

Os resultados da pesquisa, baseados no levantamento bibliográfico e no formulário online, serão apresentados a seguir. Um total de 148 pessoas participaram da pesquisa, com uma maior proporção de homens (85) em comparação com mulheres (63), conforme ilustrado na Figura 1.

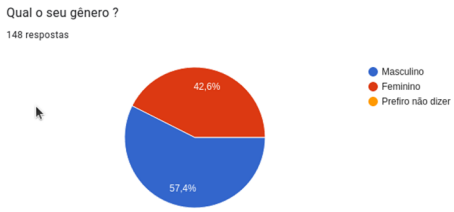

Fig. 1. Gênero dos participantes

Ainda sobre os participantes da pesquisa, o grupo etário mais frequente foi de 18 a 29 anos. A maioria dos participantes tinha ensino médio completo e superior incompleto, representando 87,2% dos indivíduos.

Em relação ao uso de antivírus no celular, mais da metade dos participantes não utilizam antivírus, conforme a Figura 2. Isso é preocupante, pois a ausência de antivírus pode deixar os usuários vulneráveis a golpes e novas técnicas de roubo de dados.

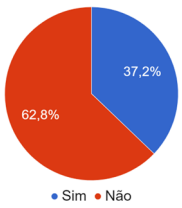

Fig. 2. Utilização de antivírus no dispositivo

O uso de software antivírus pode detectar irregularidades nos arquivos e aplicativos instalados, além de alertar sobre possíveis ameaças. Embora não ofereça proteção completa, o antivírus ajuda a evitar muitas ameaças.

Sobre a troca de senhas, muitos participantes não realizam a troca frequente de suas senhas, conforme a Figura 3. Isso pode deixá-los vulneráveis a técnicas como phishing ou keyloggers, que capturam e descobrem senhas.

Trocar senhas frequentemente ajuda a manter o dispositivo seguro, impedindo que invasores acessem serviços mesmo que tenham obtido a senha anterior.

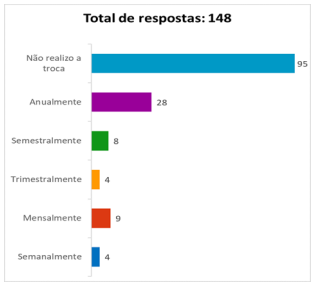

Fig. 3. Frequência de troca de senhas

De acordo com a Figura 4, sobre os locais onde as pessoas armazenam as senhas, os usuários que memorizam as senhas estão mais seguros contra roubo de dados. No entanto, memorizar várias senhas pode ser difícil, e uma solução seria o armazenamento de senhas na nuvem, que oferece proteção adicional através de criptografia.

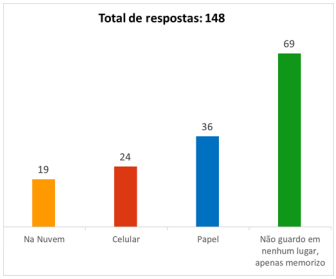

Fig. 4. Armazenamento das senhas

Sobre métodos de bloqueio e desbloqueio utilizados no dispositivo, os participantes preferiram marcar mais de uma opção. O uso da biometria foi o mais comum, seguido por senhas alfanuméricas, padrões de desenho, autenticação de dois fatores, reconhecimento facial e leitor de íris.

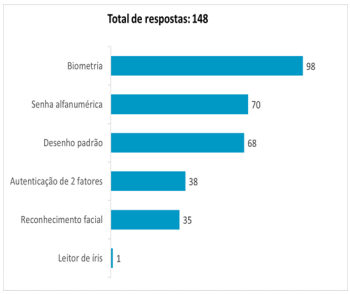

Fig. 5. Métodos de bloqueio e desbloqueio

Os resultados mostram que a maioria dos usuários mantém seus dispositivos móveis seguros, utilizando métodos de bloqueio que ajudam a proteger seus dados pessoais.

Quando questionados sobre a utilização de wi-fi público, 78 pessoas informaram que utilizam, enquanto 70 não utilizam, conforme a Figura 6. Redes wi-fi públicas podem representar perigos, como a criação de redes falsas por hackers para capturar dados dos usuários.

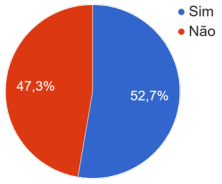

Fig. 6. Utilização de wi-fi público

Por último, a maioria dos entrevistados não se sente totalmente segura mesmo com ferramentas e mecanismos de proteção, conforme a Figura 7. Isso sugere uma desconfiança nos métodos de segurança disponíveis.

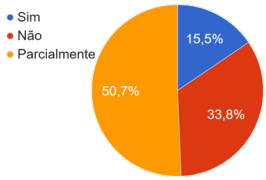

Fig. 7. Proteção com os recursos de segurança oferecidos no smartphone

IV. Considerações Finais

Após as análises e discussões das respostas do formulário, conclui-se que grande parte dos participantes não segue os padrões de segurança recomendados para dispositivos móveis. Embora muitos demonstrem conhecimento sobre o tema e os riscos associados à falta de segurança, ainda há uma lacuna significativa na adoção de práticas adequadas de proteção. Isso destaca a necessidade de maior educação e conscientização sobre segurança da informação. Além disso, é essencial que os usuários sejam informados sobre as melhores práticas de segurança e incentivados a adotá-las para proteger seus dados pessoais e profissionais.

Referências

[1] BERTOLI, Sandra Maria de Souza. *Guia de segurança para dispositivos móveis: hardware, software e comportamento*. 2014. 77 f. Trabalho de Conclusão de Curso (Graduação) – Universidade Tecnológica Federal do Paraná, Curitiba, 2014. Disponível em: http://repositorio.utfpr.edu.br/jspui/handle/1/9810. Acesso em: 09 jun. 2022.

[2] BOTTCHER, G., & GRAFF, S. *Segurança da informação: Como prevenir roubo de dados pessoais. Uma abordagem socioeducativa*. Extensão Tecnológica: Revista De Extensão Do Instituto Federal Catarinense, (3), 89 - 92. Disponível em: http://publicacoes.ifc.edu.br/index.php/RevExt/article/view/101. Acesso em: 20 mai. 2022.

[3] CABRAL, Juliana Pereira; PONTES, Herleson Paiva. *Segurança em Dispositivos Móveis: Um Estudo Sobre a Adoção de Boas Práticas para Proteção em Celulares*. In: SEMINÁRIO INTEGRADO DE SOFTWARE E HARDWARE (SEMISH), 48, 2021, Evento Online. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2021. p. 58-68. ISSN 2595-6205. Disponível em: https://sol.sbc.org.br/index.php/semish/article/view/15807/15648. Acesso em: 08 jun. 2022.

[4] CAVALCANTI, K. R. P. Uma solução integrada para a melhoria da segurança de dispositivos móveis baseada na plataforma Android, 2016.

[5] CERT.br. *Cartilha de Segurança para Internet, fascículo: Dispositivos móveis*. São Paulo: Comitê Gestor da Internet no Brasil, 2020. Disponível em: https://cartilha.cert.br/fasciculos/dispositivos-moveis/fasciculo-dispositivos-moveis.pdf. Acesso em: 06 jun. 2022.

[6] CERT.br. *Cartilha de Segurança para internet fascículo, fascículo: Códigos Maliciosos*, 2020. Disponível em: https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acesso em: 14 jun. 2022.

[7] ESET. *Qual é a importância do antivírus para celular? Entenda!*. Disponível em: https://www.eset.com/br/artigos/antivirus-para-celular/. Acesso em: 21 jun. 2022.

[8] ISFER, Andressa. *Quais os riscos de uma rede wi-fi aberta e como se proteger*. Disponível em: https://www.oficinadanet.com.br/seguranca/28096-quais-os-riscos-de-uma-rede-wi-fi-aberta-e-como-se-proteger. Acesso em: 11 jul. 2022.

[9] MESQUITA, Pablo. Desafios da forense em dispositivos móveis. Gestão da Segurança da Informação - Unisul Virtual, 2018.

[10] ROSHANDEL, R., ARABSHAHI, P. and POOVENDRAN, R. (2013) "LIDAR: A Layered Intrusion Detection and Remediation Framework for smartphones", In Proceedings 4th ACM Sigsoft symposium on Architecting critical systems, p. 27-32

[11] SANTINO, Renato. *Wi-Fi público: entenda os riscos de usar o Wi-Fi fora de casa*. Disponível em: https://olhardigital.com.br/2019/07/19/seguranca/wi-fi-publico-entenda-os-riscos-de-usar-o-wi-fi-fora-de-casa/. Acesso em: 19 jun. 2022.

[12] SURFSHARK. *Data breach statistics by country in 2021*. Disponível em: https://surfshark.com/blog/data-breach-statistics-by-country-in-2021. Acesso em: 22 jun. 2022.