JOURNAL OF APPLIED SCIENCE AND SOCIAL SCIENCE
eISSN 2229-3113 pISSN 2229-3205
Volume 14 Issue 12, December 2024
Impact factor: 2019: 4.679 2020: 5.015 2021: 5.436, 2022: 5.242, 2023: 6.995, 2024 7.75

CYBERATTACKS ON TELEGRAM AND THE MITIGATION OF THE ISSUE

Sherzod Chulliev
A senior at high school 29th, Bukhara city,
Bukhara region, Uzbekistan
Independent research
Email: sherzodchulliyev33@gmail.com

Abstract: The surge in the use of the Internet throughout the world, along with bringing numerous benefits to people, has started posing threats to users' data, especially their money. This research aims to pay particular attention to the most common cyberthreats on the increasingly more popular social media platform Telegram (Singh, 2024). While Telegram's use of end-to-end encryption provides users with strong protection against information leaks, this same feature also makes it more difficult to identify and prevent online threats, leaving general people at risk of falling for these attacks. By examining well-known sources such as Google Scholar, ScienceDirect, Springer, and IEEE, one can observe the relative scarcity of research on this specific topic. I, with my research paper, aim to alleviate this issue to a certain extent.

Introduction

To realize the importance of establishing proper defense against cyberattacks, the general cost of cyberattacks should be considered. Although the true cost of attacks cannot be accurately measured, the projections for 2024 show a massive $9.5 trillion (Cybersecurity Ventures, 2024) compared to $6.9 billion in 2021 (Federal Bureau of Investigation, 2021). Researchers believe that these losses are further expected to rise, especially now that AI is being involved to target users' data more effectively (Benjamin, 2024).

Now, in the case of Telegram, users can exchange information via end-to-end encryption. This method is claimed to be used by major social media companies on platforms like WhatsApp, Facebook Messenger, Instagram, Telegram, Threema, Snapchat, etc. The major benefit of encrypted messaging is that no outsider can observe the chat in any way. This allows for safe, uninterrupted communication by offering protection from third-party surveillance and resistance to tampering (IBM, n.d.).

This method might, on the surface, look perfect for the protection of data, but it makes it vulnerable to trace criminals since the companies have no control over their users' data. According to IBM, E2EE hinders law enforcement agencies from preventing and detecting criminal activities, such as terrorism, cybercrime, and child exploitation (IBM, n.d.).

The following parts of this paper are dedicated to exploring the specific cases of cyberattacks in the context of Telegram, as well as providing solutions to be safe from them.

Methodology

This study employs a combination of various methods. The paper focuses on the survey results from a relatively small yet diverse group of Telegram users. Participants in the survey represent various groups of people from Uzbekistan and Kazakhstan: divided according to ages 15-25, 25-35, and 40+. This study can only represent the cases inside Central Asia for the most part. Over 70% of Uzbekistan's population uses Telegram actively (Daryo, 2024). For reasons such as varying technological proficiency, differences in usage patterns, and the strategies

JOURNAL OF APPLIED SCIENCE AND SOCIAL SCIENCE
eISSN 2229-3113 pISSN 2229-3205
Volume 14 Issue 12, December 2024
Impact factor: 2019: 4.679 2020: 5.015 2021: 5.436, 2022: 5.242, 2023: 6.995, 2024 7.75

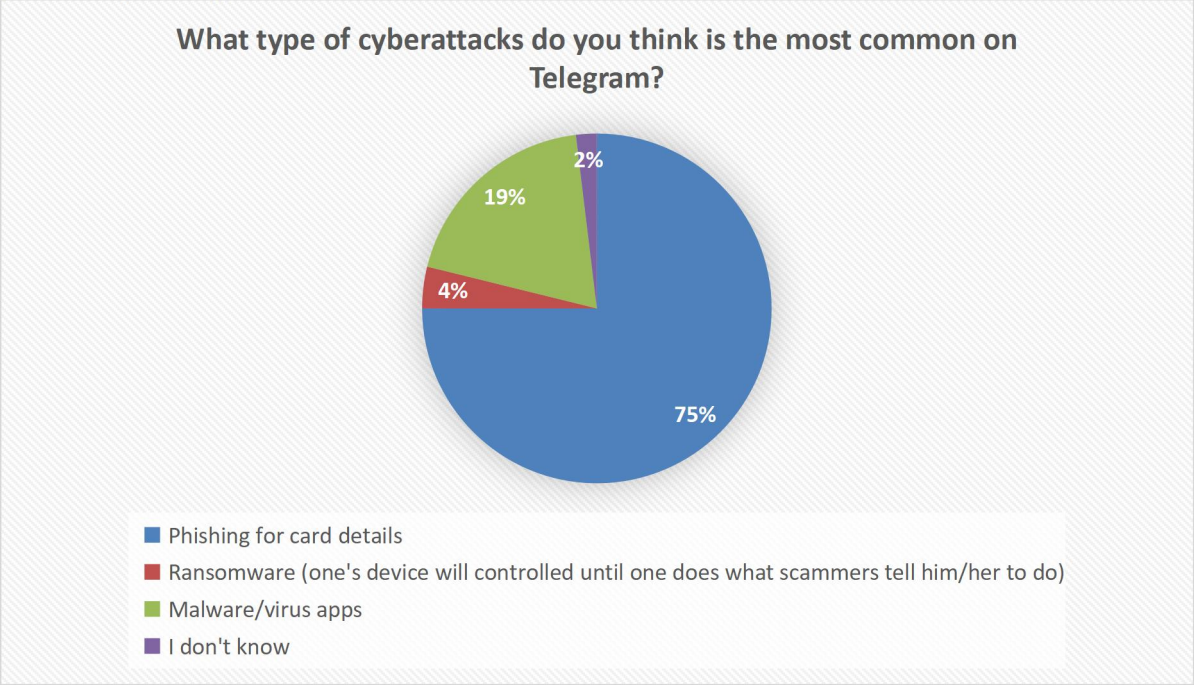
scammers utilize to target various age groups, the study divides the population by age groups. The survey includes closed and open-ended questionnaires.

Furthermore, data have been collected from various official sources to prevent the likelihood of overgeneralization in the research. This supplementary data provided a contextual backdrop against which the survey results were compared, ensuring a comprehensive understanding of scam tactics across different demographics.

Common ways hackers use to scam everyday users of Telegram

A. Phishing scams.

By far, phishing scams are the most common method scammers use to trick people into sending sensitive debit card data and stealing all the money at once. In order not to get caught, they withdraw money and immediately convert to cryptocurrency like Bitcoin. Over the past few years, different persuasive methods have been in use: (Kun.uz, 2022), (Kun.uz, 2024), etc. In the survey as well, phishing for card details was found to be the most common overall:



B. Ransomware/malware

By definition, ransomware refers to 'software that is used to demand money from an individual or organization by blocking access to applications or files on a computer system until a sum of money is paid.' Scammers on Telegram typically send a file to a random user stating that they have won a particular giveaway; to get the gift, they ask the user to open the app. Once opened, the pre-installed virus gets control of the device and acquires all the user information. The virus then sends the link to everyone in the user's contacts without asking (Kun.uz, 2024).

C. Impersonation

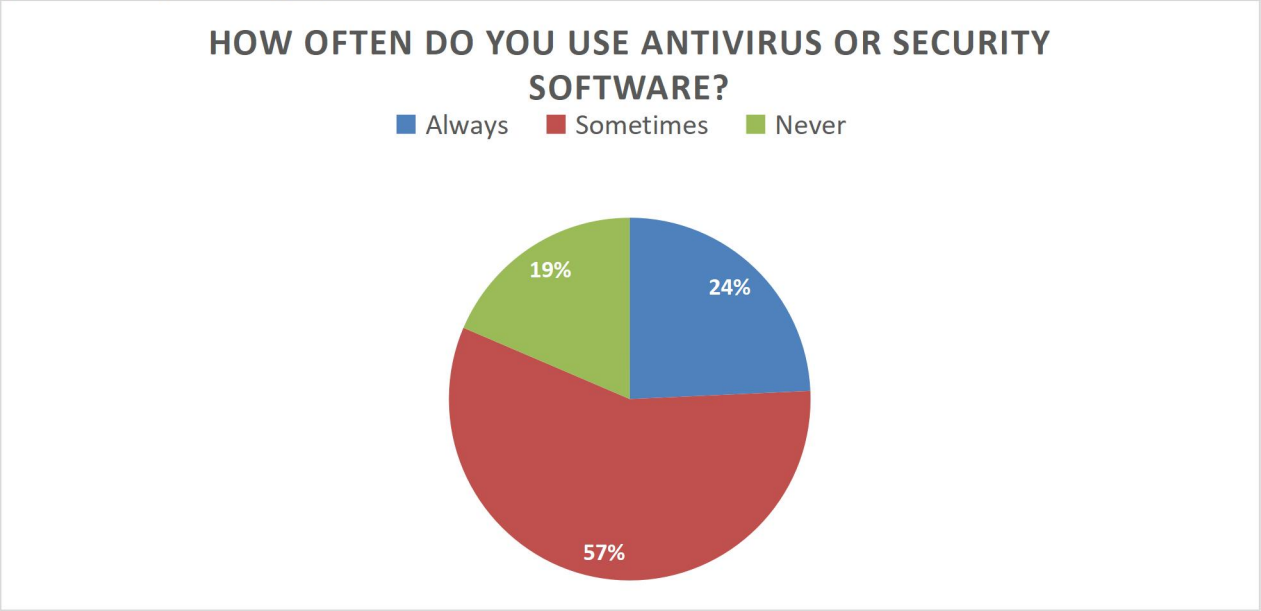
In this case, scammers observe a particular user by collecting enough information about their friends, family members, or relatives; once done, fraudsters impersonate their friends' accounts and ask for money from the user, saying they need urgent help. It has existed for a

JOURNAL OF APPLIED SCIENCE AND SOCIAL SCIENCE
eISSN 2229-3113 pISSN 2229-3205
Volume 14 Issue 12, December 2024
Impact factor: 2019: 4.679 2020: 5.015 2021: 5.436, 2022: 5.242, 2023: 6.995, 2024 7.75

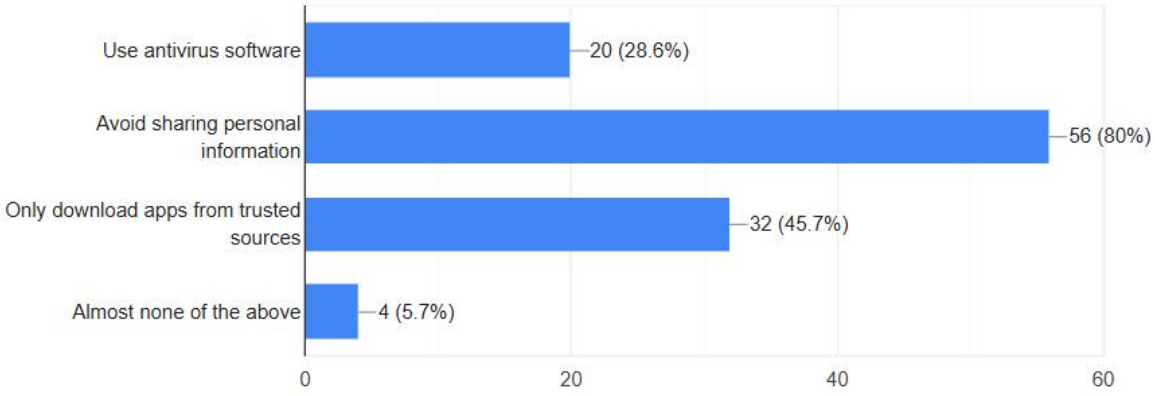
while on other social media platforms now (Instagram, n.d.) , and it is getting popular on Telegram too.

Solutions to prevent scams

Enough information has been given about the current cost of cyberattacks and the importance of preventing them. However, only 24% of them said they always had protection from cyberattacks, and a large portion does it sometimes:



When asked what steps they were currently taking to protect their online information, the chart results were this:



Apparently, most of users know that they should avoid sharing personal information, but they are somewhat unaware of the common attacks scammers use to acquire user information indirectly. Therefore, I argue that there seems to be a large gap between knowing what not to do and implementing this knowledge. There may be numerous factors associated with, which this paper does not go into detail, but minimizing this gap could prevent further financial losses, data breaches, and other forms of cybercrime. Teaching the public to implement defensive strategies like verifying the authenticity of any message before opening it, using two-factor verification

JOURNAL OF APPLIED SCIENCE AND SOCIAL SCIENCE
eISSN 2229-3113 pISSN 2229-3205
Volume 14 Issue 12, December 2024
Impact factor: 2019: 4.679 2020: 5.015 2021: 5.436, 2022: 5.242, 2023: 6.995, 2024 7.75

and strong passwords will be a significant step in mitigating these issues.

Conclusion

The research aimed to identify the most prevalent cyberattacks on Telegram. The research findings suggest that phishing for card details, ransomware/malware virus apps, and impersonation are by far the most common methods employed to exploit the general public. A number of sources were used in addition to a public survey to reach these conclusions. As part of a solution, the survey results found a significant gap between people's general awareness and a lack of implementation of this knowledge when it preventing the attacks.

Nevertheless, this research paper does not claim to be fully irreproachable by any means. The research findings might not apply to other countries other than those in Central Asia since the survey did not include respondents from other countries. The research could not find any official Telegram reports on Cyberattacks related to Uzbekistan. The scope of research could be increased with the addition of more sources when Telegram starts to focus on gathering data. Future researchers can address these limitations when there is more official data available on Cyberattacks in Uzbekistan.

References

1. Benjamin, V. (2024, October 18). AI-driven cyberattacks more sophisticated and scalable, but ASU expert offers solutions. Retrieved from ASU News: https://news.asu.edu/20241018-science-and-technology-aidriven-cyberattacks-more-sophisticated-and-scalable-asu-expert

2. Cybersecurity Ventures. (2024). Cybercrime to Cost the World $9 Trillion Annually in 2024. Retrieved from Cybersecurity Ventures: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

3. Daryo. (2024). Over 70% of Uzbekistan's 37 mn population utilizes Telegram - Pavel Durov. Retrieved from Daryo: https://daryo.uz/en/2024/06/30/over-70-of-uzbekistans-37-mn-population-utilizes-telegram-pavel-durov#:~:text=Telegram%20%2D%20Pavel%20Durov-,Over%2070%25%20of%20Uzbekistan's%2037%20mn%20population%20utilizes%20Telegram%20%2D%20Pavel,recent%20visit%20to%20

4. Federal Bureau of Investigation. (2021). 2021 Internet Crime Report. Retrieved from Internet Crime Complaint Center (IC3): https://www.ic3.gov/AnnualReport/Reports/2021_IC3Report.pdf

5. Kakhramonovna, K. S. (2024). THE ROLE OF SPIRITUAL EDUCATION IN THE DEVELOPMENT OF THE NEW UZBEKISTAN. *JOURNAL OF INTERNATIONAL SCIENTIFIC RESEARCH*, *1*(3), 84-102.

6. Jurakulovich, S. J. (2024). THE ROLE OF SPIRITUALITY IN THE IMPLEMENTATION OF THE DEVELOPMENT STRATEGY OF THE NEW UZBEKISTAN. *Ethiopian International Journal of Multidisciplinary Research*, *11*(11), 307-311.

7. Jurakulovich, S. J. (2024). GLORIFYING MAN AND INCREASING HIS VALUE IS THE MAIN GOAL OF THE THIRD RENAISSANCE. INTERNATIONAL MULTIDISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT SJIF 2019: 5.222 2020: 5.552 2021: 5.637 2022:5.479 2023:6.563 2024: 7,805 eISSN :2394-6334 https://www.ijmrd.in/index.php/imjrd Volume 11, issue 11 (2024). Pp. 389-394.

JOURNAL OF APPLIED SCIENCE AND SOCIAL SCIENCE
eISSN 2229-3113 pISSN 2229-3205
Volume 14 Issue 12, December 2024
Impact factor: 2019: 4.679 2020: 5.015 2021: 5.436, 2022: 5.242, 2023: 6.995, 2024 7.75

8. IBM. (n.d.). What Is End-to-End Encryption? Retrieved from IBM: https://www.ibm.com/topics/end-to-end-encryption

9. Instagram. (n.d.). Instagram. Retrieved from Report an Impersonation Account on Instagram: https://help.instagram.com/contact/636276399721841

10. Kun.uz. (2022). Warning: Scammers are circulating a false message on Telegram that people are being distributed money. Retrieved from Kun.uz: https://kun.uz/en/news/2022/11/22/warning-scammers-are-circulating-a-false-message-on-telegram-that-people-are-being-distributed-money

11. Kun.uz. (2024). 18-year-old youngster arrested for spreading malicious virus programs on Telegram. Retrieved from https://kun.uz/en/news/2024/01/31/18-year-old-youngster-arrested-for-spreading-malicious-virus-programs-on-telegram

12. Kun.uz. (2024). Law enforcement's inaction: The growing threat of Telegram scams in Uzbekistan. Retrieved from Kun.uz: https://kun.uz/en/news/2024/07/24/law-enforcements-inaction-the-growing-threat-of-telegram-scams-in-uzbekistan

13. Singh, S. (2024, August 29). Telegram Statistics (2024) — Users & Revenue Data. Retrieved from Demandsage: https://www.demandsage.com/telegram-statistics/