International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-11 Issue-6, March 2023

Cybercrime Landscape and Changes During the Pandemic in Division 4 (West North Central)

Trang Thi Thu Horn, Mahmoud Yousef

Abstract*: Since its existence in December 2019, COVID-19 has significantly impacted different sectors of the economy in both the physical and digital worlds. In cyberspace, the Covid-19 pandemic has changed the cybercrime landscape. In this study, we focus on data collected by the Federal Bureau of Investigation (FBI) in the West North Central (Division 4) region. Data was collected for each state for different types of crimes and was divided into various age groups. Non-payment and non-delivery have the highest number of victims compared to other types of crimes. Moreover, over the past five years, the over-60 age group had the highest number of victims in Kansas, Missouri, South Dakota, and Minnesota. However, the number of elderly cybercrime victims ranked second compared to other age groups in Iowa and Nebraska and third in North Dakota.

***Keywords*: Cybercrimes, Elderly Fraud, COVID-19 Impact.**

I. INTRODUCTION

Cyber security began in the 1970s when a researcher named Bob Thomas created Creeper, a computer program that could move across ARPANET's network; meanwhile, Ray Tomlinson wrote the program Reaper which chased and deleted Creeper [1]. Cybersecurity has been increasingly important due to the significant increase in our reliance on computer systems in our daily activities, whether work-related or personal life related. COVID 19 started in December of 2019, it quickly became a crisis causing the government to shut down, and millions of people were requested to stay home and work from home. In February 2023, it was reported that over 6.8 million people had died so far from the coronavirus COVID-19 outbreak, and there have been more than 753 million confirmed cases [2]. The COVID-19 pandemic causes a significant loss of human life worldwide, poses challenges, and disrupts our society. In times of crisis, a sharp increase in cybercrimes is expected. Cybersecurity threat has increased significantly since the start of COVID-19. As it is such an unprecedented event, individuals have challenges recognizing and protecting themselves from cyberattacks in cyberspace. While individuals are trying to protect their health and deal with financial issues, the attacker took advantage of the situation to make money from cybercrimes. They carry out different types of attacks, including phishing, spoofing, extortion, confidence fraud/romance, tech support, and other types of internet base attacks to target the vulnerable victims in our societies [3]. Cybercrime doesn't have such traditional boundaries as a traditional crime. The traditional crime investigation, detecting, and reporting methods fail in virtual environments [4], making it harder to take down cybercrime. This paper will explore the Cybersecurity landscape and changes during the pandemic in the West North Central region (division 4), which includes Kansas, Iowa, Missouri, North Dakota, South Dakota, Minnesota, and Nebraska.

II. BACKGROUND

In the past, several pandemics occurred, such as the Spanish Flu, Bubonic Plague, and Small-Pox that infected and killed millions of people [5]. However, since back then, the Internet and technology were not as developed as nowadays, the pandemic created a more isolated and less of a global impact due to not having the capability to travel a far distance and communicate across the globe. In 2014, the Ebola outbreak had an impact on cybersecurity. Email scams and fishing campaigns used Ebola as a social engineering theme, which was then identified as the most widespread attack vector [6]. The attacks aimed to infect users' devices and steal passwords and personal information. However, the impact was limited to the West Africa region and did not spread globally as COVID-19. The COVID-19 pandemic has caused a striking loss of lives worldwide and unprecedented challenges to public health, work, and the food system [7]. Scammers take advantage of the situation and carry out phishing attacks to exploit public fear, concerns, and curiosity about the deadly virus. An example is COVID-19 phishing email. The phishing email generally claims to be from legitimate organizations (e.g., health organizations, employers, and charitable organizations) and asks the victim to click on the attachment for information on the latest statistics, policy procedures to address the risk or help the victim of the virus. Once the victims click on the malicious link or attachment, malicious software will be downloaded to their devices. Malicious websites containing maps and dashboards related to covid were also popular when it first started. Another factor that contributes to the increase in cybercrimes is the human factor. Humans are often considered the weakest link in cybersecurity; therefore, they are often the target of cyberattacks [8]. In a pandemic, people are urged to be informed and have significant concerns about their job situations and health issues, making them easy targets for cybercrimes, especially social engineering.

Manuscript received on 20 February 2023 | Revised Manuscript received on 24 February 2023 | Manuscript Accepted on 15 March 2023 | Manuscript published on 30 March 2023.
*****Correspondence Author(s)
Trang Thi Thu Horn*, Department of Computer Science and Cybersecurity, College of Health Science and Technology, University of Central Missouri, Warrensburg, USA. Email: thorn@ucmo.edu. ORCID ID: https://orcid.org/0000-0003-0399-4517.
Dr. Mahmoud Yousef, Department of Computer Science and Cybersecurity, College of Health Science and Technology, University of Central Missouri, Warrensburg, USA. Email: yousef@ucmo.edu. ORCID ID: https://orcid.org/0009-0009-1153-620X.

Social engineering refers to "human hacking" that utilizes manipulation technique to exploit human error to gain access to information and valuables [9]. Social engineering attacks are considered the most dangerous and have a high chance of success. In addition, online activities increased significantly during the pandemic. Organizations and schools requested their employees to work from their homes and students to study remotely. Individuals must maintain social distancing for essential activities such as grocery shopping, visiting the doctors, etc., which cause increased needs for online grocery shopping, virtual doctor appointments, etc. Consequently, society entirely depended on technology and the Internet for work, study, communication, entertainment, and social interaction, creating promising hunting fields for attackers during the pandemic. There was about 1001 frequency of data breaches, with a total number of victims of 155.8 million people in 2020 [10]. This paper will study the data collected by the Internet Crime Complaint Center, a Federal Bureau of Investigation division, regarding cybercrime in each state in different years. The data is collected by crime types and divided into various age groups for each state.

III. CYBERSECURITY THREAT DURING THE PANDEMIC

The pandemic created a perfect landscape for attackers to perform their attacks. The main reasons that contribute to the rise in the number of cyber-attacks are listed below: First, our society had become so dependent on technology and the Internet due to the requirement to maintain social distancing, work from home, or virtual learning when the pandemic started. Many transactions containing our sensitive or essential data were transferred over the Internet, making it a rich field for criminals to target. Second, the concept of working and studying from home has been widely adopted since the pandemic, which poses many challenges regarding cybersecurity. Especially when the pandemic started, the sudden shift to remote working and learning caused difficulties for individuals needing more preparation time. Third, humans are more curious and urged to look for or check any information sent to them, especially when they are worried, concerned, or have doubts. When people are desperate for information, people are easier to be misled and enticed to click on malicious links [11]. Fourth, during the pandemic, individuals spent most of their daily time either working, studying, communicating, or entertaining via online services, websites, and applications, making them more susceptible to cyber-attacks. Lastly, remote work and virtual study made individuals who were unaware of cybersecurity or lack of cybersecurity knowledge easy targets for attackers.

IV. UPSURGE IN CYBERCRIME AND DIFFERENT TYPES OF ATTACKS DURING THE PANDEMIC IN DIVISION 4 (WEST NORTH CENTRAL STATES)

In March 2020, the pandemic hit the United States, posing significant changes in social norms, including quarantine requirements, product shortages, business closures, or struggling to survive, significantly impacting the economy [12]. In a time of crisis, it is expected that the number of crimes will increase. In 2020, the Internet Crime Complaint Center (IC3) received a record-high number of complaints from the American public, 791,790, with a loss of revenue over 4.1 billion dollars [13]. The total number of victims counts for the West North Central States (Division 4) region increased significantly from 2019 to 2020 when the pandemic started. Specifically, we saw an increase of 67.32% in the total number of victims counts in division 4.

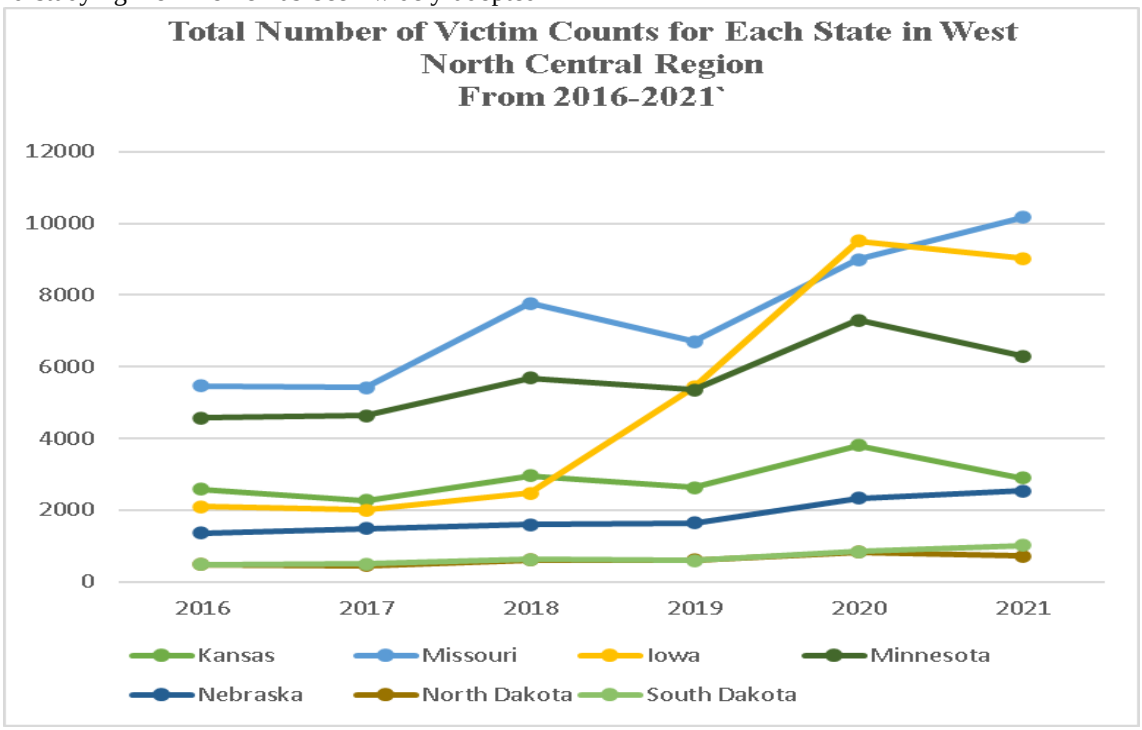

Figure 1: Total Number of Victim Counts for Each State in Division 4 From 2016 -2021

Retrieval Number: 100.1/ijrte.F74910311623
DOI: 10.35940/ijrte.F7491.0311623
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Specifically, for each state in Division 4, there is an increase of 83.88% in Iowa, 75.48% in Kansas, 56.04% in Minnesota, 60.54% in Missouri, 60.44% in Nebraska, 55.42% in North Dakota, 64.27% in South Dakota.

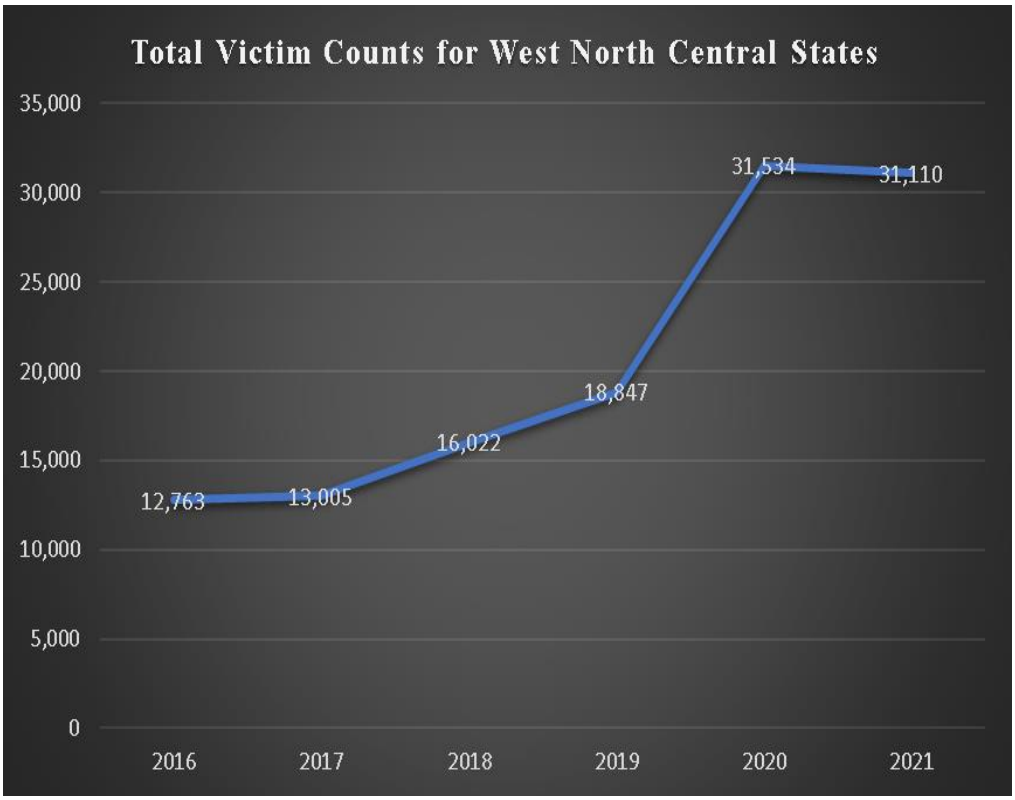

Figure 2: Total Number of Victim Counts for Division 4 From 2016 -2021

In 2021, despite a slight decrease in total victim counts in West North Central states, it still showed an increase of 65.07% compared to 2019.

Various types of attacks are carried out during the pandemic. According to the dataset collected by IC3, the common types of attacks in division 4 include non-payment/non-delivery, identity theft, extortion, personal data breach, tech support, confidence fraud/romance, BEC/EAC, spoofing, phishing/vishing/smishing/pharming. These types of crime are defined as follows:

• Non-payment/non-delivery cybercrimes refer to the type of crime in which purchase goods and services are sent, but no payment is rendered (non-payment), or payments are sent, but no goods or service was received (non-delivery) [14].

• Identify theft refers to the act of stealing personal identifying information to commit fraud or crimes [14].

• Extortion is a crime type in which the attacker uses intimidation and undue authority to extract money and property illegally [14].

• A personal data breach happens when individuals' personal information is leaked, used, transmitted, exposed, copied, or stolen by unauthorized individuals [14].

• In a tech support scam, the criminal poses as a technical/customer support or service resolving issues such as compromised email, bank account, infected computer, etc., to defraud unsuspecting individuals [14].

• In a confidence fraud/romance scam, the victim believes they are in a relationship which can be a family, friend, or romantic relationship. They are tricked into sending money, information, and valuable items to the criminal or assisting the criminal in laundering money or items [14].

• BEC/EAC is the short form of Business Email Compromise/ Email Account Compromise scam. BEC targets business working with foreign suppliers or partners and often perform wire transfer payment [14]. Meanwhile, EAC is similar to BEC; instead, the perpetrator targets individuals (Federal Bureau of Investigation-Internet Crime Complaint Center, 2020). These scams are performed through compromised email accounts to conduct unauthorized funds transfers using social engineering [14]

• In a spoofing attack, contact information is falsified and appears to be a legitimate source to mislead and gather information [14].

• Phishing/vishing/smishing/pharming refers to using means such as unsolicited email, messages, or phone calls that appear to be from legitimate sources requesting information or login credentials [14].

During the pandemic time from 2020 -2021, among these widespread crimes, non-payment/non-delivery has the highest number of victim counts in the West North Central states (Division 4). The pandemic lockdown, capacity restrictions, and individuals changing their shopping habits (reluctance to shop in person) caused a sudden increase in online shopping [15]. In fact, it was found that individuals who shop online at least once a week increased from 11.6% in 2019 to 51.2% in 2020 [15]. The scammer often pretends to be legitimate online sellers using fake websites or fake ads on legitimate retail websites [16].

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

New versions of online shopping scams utilize social media platforms to create fake online stores [16]. Scammers take advantage of social media and online advertising, and they get rid of negative reviews by disappearing and coming back up with a different name [17].

Therefore, causing challenges for consumers to identify and protect themselves from these scammers.

It is also observed that among different age groups, including under 20, 20-29, 30-39,40-49,50-59, and over 60, the elderly over 60 have the highest number of victims compared to other age groups in these states, including Kansas, Missouri, Minnesota, and South Dakota during the time periods from 2020-2021. Meanwhile, the population of age over 60 accounts for 22.2% to 23.5% of the people in these states in 2020. Specifically, the population of age 60 and over accounts for 22.2% of the total population in Kansas [18], 23.5% of the total population in Missouri [19], 22.3% of the total population in Minnesota [20], 23.3% of the total population in South Dakota [21]. These statistics raise concerns regarding cybercrime targeting the elderly, and actions are needed to protect the elderly in our society against cybercrimes.

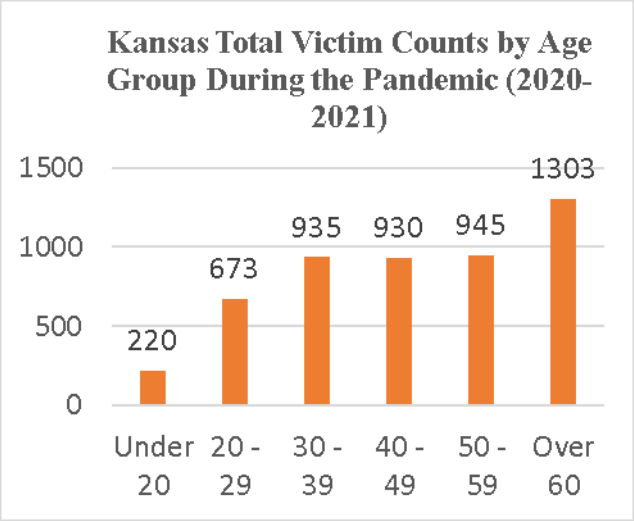

Figure 3: Kansas Total Victim Counts by Age Group During the Pandemic 2020-2021

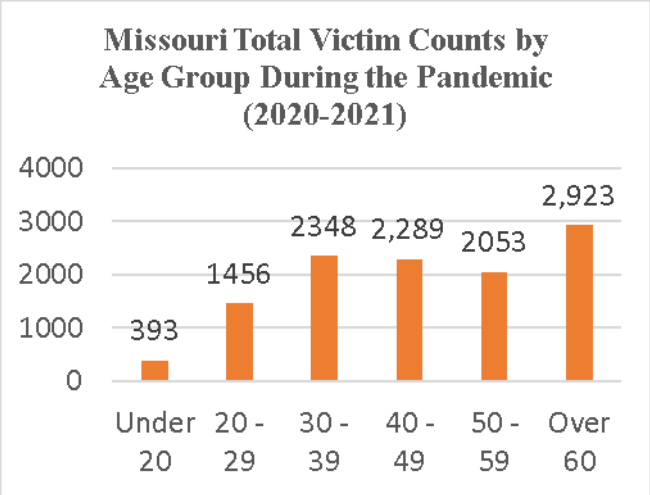

Figure 4: Missouri Total Victim Counts by Age Group During the Pandemic (2020 - 2021)

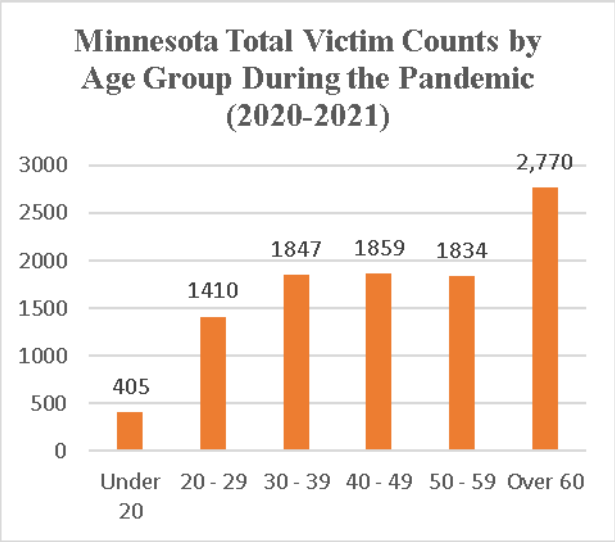

Figure 5: Minnesota Total Victim Counts by Age Group During the Pandemic (2020 - 2021)

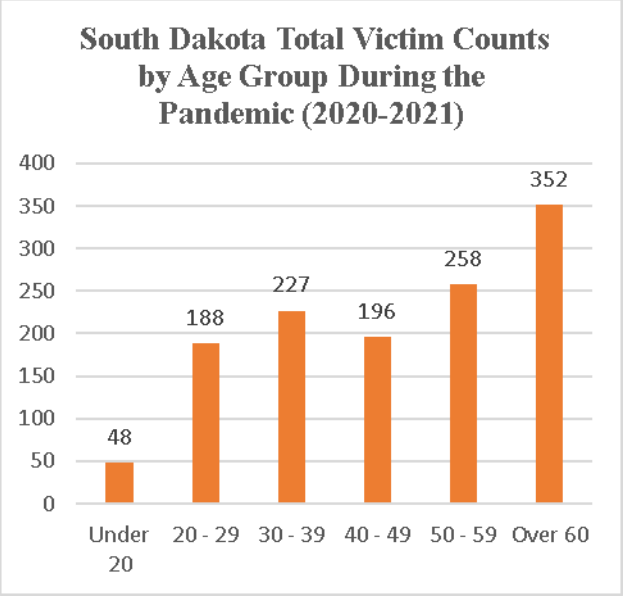

Figure 6: South Dakota Total Victim Counts by Age Group During the Pandemic (2020-2021)

Moreover, over the past five years, the over-60 age group had the highest total number of victims in Kansas, Missouri, South Dakota, and Minnesota. Meanwhile, the number of elderly cybercrime victims in Iowa and Nebraska ranked second compared to other age groups and third in North Dakota. The elderly is an attractive target for criminals since they tend to be trusting and polite; they also often have financial savings and good credit [22]. In addition, they might be seen to be less tech-savvy and less aware of various types of scams and how to spot them [23]. Furthermore, The Internet provides convenient, comfortable, and less intimidating ways to meet and connect with new people for most elderly. The common scams for victims over the age of 60 include Tech Support Fraud, confidence fraud/romance scams, lottery/sweepstakes/inheritance, government impersonation, investment, and cryptocurrency [24].

Retrieval Number: 100.1/ijrte.F74910311623
DOI: 10.35940/ijrte.F7491.0311623
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Among these crime types, confidence fraud/romance scams had the highest monetary losses in Kansas, Missouri, Minnesota, Nebraska, and South Dakota compared to other defined crime types for the elderly in 2021. Specifically, there was a total loss of $3.21 million in Kansas [25], $5.24 million in Missouri [25], $5.62 million in Minnesota [25], $856 thousand in Nebraska [25], $1.02 million in South Dakota [25] due to confidence fraud/romance scams. These concerning statistics raise the alarm for cyber attackers exploiting the vulnerable population in our society. The elderly is like everyone else who does not want to be lonely and would like to find someone to share their life with, often seeking their perfect partner after a divorce or even losing a partner [23]. Romance scammers create fake profiles to exploit older adults' loneliness to get money [26]. Romance scammers have all sorts of believable stories to take advantage of the victim's "heartstring," including pleas for help with financial and health crises one after another. These scammers often drag on for a long time, bilking the victim a lot of money before those scams are reported. In 2021 confidence fraud/romance scams had the highest number of victims in North Dakota compared to other defined crime types for the elderly. Romance scams across the nation in 2021 reached a record loss of $547 million, and North Dakota was on the top list of states with the most money lost per capita through love-themed fraud [27]. These numbers are based on reported crimes; in reality, not all cybercrime is reported due to several factors, including feeling ashamed or fearing that others think they can take care of themselves or not aware of the supporting source or know how to access them [28].

V. PROTECTING THE ELDERLY FROM CYBERCRIMES

Several countermeasures can be taken to protect the elderly from cybercrime, including the following:

- Government agencies and community organizations can conduct outreach programs and provide educational resources and cybersecurity training to raise cybersecurity awareness among the elderly. They should be informed about popular crime types targeting the elderly, aware of best practices when using the internet, such as using strong passwords, installing antivirus, updating software, and how to recognize popular scams targeting the elderly such as requests for money, requests for sensitive personal and financial information. The amount of information posted on social media should be minimal. The more information posted on social media, the easier for the attacker to target the victims.
- The elderly should be encouraged to sign up for alerts for their financial accounts and let another family member get "view only" access as a second set of eyes in case of malicious transactions.
- Dating apps and websites can implement policies and procedures to verify user identities and detect suspicious behaviors. In addition, they should also warn users about the risks of sharing sensitive personal and financial information or sending money to someone they have never met in person.
- Providing support to the elderly who have been victimized is critical. Community organizations and government agencies can offer counseling services and financial assistance to help victims recover from the emotional and financial impacts of the fraud. Family members and caregivers can also play an essential role in supporting the elderly victims of cybercrimes by providing emotional support and helping them access the necessary resources.
- Finally, encouraging the elderly to report cybercrimes so law enforcement agencies can act against cybercriminals, including investigation, prosecution, and international cooperation to track down and extradite cybercriminals.

VI. CONCLUSION

The pandemic has changed our society in such a unique way. Cybersecurity is one of the areas that are significantly impacted by the pandemic. Fears, concerns, and confusion create a perfect situation for the attacker to perform various social engineering attacks. The number of victim counts increased significantly during the pandemic compared to before the pandemic. The total number of elderly victims is concerning, raising the alarm to protect our elderly in cyberspace—more countermeasures or policies are needed to protect the elderly from cybercrimes. In addition, cybersecurity training should be provided to the larger population, especially the elderly, to help them be well prepared and protect themselves from cybercrimes.

DECLARATION

Funding/ Grants/ Financial Support	No, we did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	The research utilized publicly available data provided by the Internet Crime Complaint Center (IC3)
Authors Contributions	Trang Thi Thu Horn and Dr. Mahmoud Yousef developed the topic. Trang T. Horn performed the computation of data and wrote the manuscripts. Dr. Yousef supervised, reviewed the finding of the work, and provided feedback and suggestions as needed. Both authors discussed the results and contributed to the final manuscript.

REFERENCES

1. Geeksforgeeks, "History of Cyber Security," 22 6 2022. [Online]. Available: https://www.geeksforgeeks.org/history-of-cyber-security/. [Accessed 4 2 2023].
2. World Health Organization [WHO], "WHO Coronavirus (COVID-19) Dashboard," [Online]. Available: https://covid19.who.int/.

3. Internet Crime Complaint Center (IC3), "Annual Reports," [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2021State/StateReport.aspx. [Accessed 2 2 2023].
4. Federal Bureau of Investigation, "Testimony," [Online]. Available: https://archives.fbi.gov/archives/news/testimony/the-fbis-perspective-on-the-cybercrime-problem. [Accessed 3 2 2023].
5. F. Mouton and A. Goning, "COVID-19: Impact on the Cyber Security Threat Landscape," Research Gate, p. 6, 2020.
6. CyberPeace Institute, "A Brief History of Cyberattacks: From Ebola to COVID-19," 26 3 2020. [Online]. Available: https://cyberpeaceinstitute.org/news/2020-03-26-a-brief-history-of-infodemics-from-charlie-hebdo-to-ebola-and-covid-19/. [Accessed 4 2 2023].
7. World Health Organization, "Impact of COVID-19 on people's livelihoods, their health and our food systems," 13 10 2020. [Online]. Available: https://www.who.int/news/item/13-10-2020-impact-of-covid-19-on-people's-livelihoods-their-health-and-our-food-systems. [Accessed 2 2 2023].
8. SHRM, "The Weakest Link in Cybersecurity," SHRM, 21 10 2021. [Online]. Available: https://www.shrm.org/hr-today/news/all-things-work/pages/the-weakest-link-in-cybersecurity.aspx. [Accessed 2 2 2023].
9. Kaspersky, "What is Social Engineering?," [Online]. Available: https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering. [Accessed 2 2 2023].
10. M. Alawida, A. Omolara, O. Abiodun and M. Al-Rajaba, "A deeper look into cybersecurity issues in the wake of Covid-19: A survey," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 10, p. 8176–8206, 2022. [CrossRef]
11. American Bar Association, "The Importance of Cybersecurity Amid COVID-19," [Online]. Available: https://www.americanbar.org/groups/law_practice/resources/cybersecurity_covid19/#:~:text=Increased%20Cyber%20Risks&text=When%20people%20become%20desperate%20for,to%20click%20on%20malicious%20links... [Accessed 7 2 2023].
12. S. Roman, S. Cooke-Hull, M. Dunfee, M. Flaherty, J. Haskell, V. Holland, C. Jackson and C. and Shevlin, "The Coronavirus Pandemic's Economic Impact," 28 7 2022. [Online]. Available: https://www.census.gov/library/publications/2022/econ/coronavirus-pandemics-economic-impact.html. [Accessed 2 2 2023].
13. Internet Crime Complaint Center, "Internet Crime Report 2020," Federal Bureau of Investigation, 2020.
14. Federal Bureau of Investigation, "Internet Crime Report 2021," Federal Bureau of Investigation, 2021.
15. M. Young, J. Soza-Parra and G. Circella, "The increase in online shopping during COVID-19: Who is responsible, will it last, and what does it mean for cities?," Regional Science Policy and Practice, vol. 14, no. S1, pp. 162-178, 2022. [CrossRef]
16. W. Simpson, "Online Shopping Scams," [Online]. Available: https://www.fdacs.gov/Consumer-Resources/Scams-and-Fraud/Online-Shopping-Scams. [Accessed 7 2 2023].
17. E. Fletcher, "Pandemic purchases lead to record reports of unreceived goods," 1 7 2020. [Online]. Available: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2020/07/pandemic-purchases-lead-record-reports-unreceived-goods. [Accessed 7 2 2023].
18. Sixty and Me, "KANSAS AGING STATISTICS & RESOURCE GUIDE," 21 9 2020. [Online]. Available: https://sixtyandme.com/aging/kansas-aging-resource-guide/#:~:text=Kansas%20Key%20Statistics,seniors%20aged%2065%2B%20living%20alone. [Accessed 7 2 2023].
19. Sixty and Me, "MISSOURI AGING STATISTICS & RESOURCE GUIDE," 21 9 2020. [Online]. Available: https://sixtyandme.com/aging/missouri-aging-resource-guide/. [Accessed 7 2 2023].
20. S. a. Me, "MINNESOTA AGING STATISTICS & RESOURCE GUIDE," 21 9 2020. [Online]. Available: https://sixtyandme.com/aging/minnesota-aging-resource-guide/. [Accessed 7 2 2023].
21. Sixty and Me, "SOUTH DAKOTA AGING STATISTICS & RESOURCE GUIDE," 21 9 2020. [Online]. Available: https://sixtyandme.com/aging/south-dakota-aging-resource-guide/. [Accessed 7 2 2023].
22. FBI, "Elder Fraud," [Online]. Available: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/elder-fraud. [Accessed 7 2 2023].
23. S. Maris, "Why Seniors are Falling Victim to Romance Scammers," 20 7 2021. [Online]. Available: https://www.eyeonannapolis.net/2021/07/why-seniors-are-falling-victim-to-romance-scammers/. [Accessed 7 2 2023].
24. Federal Bureau of Investigation, "Elder Fraud Report," Federal Bureau of Investigation, 2021.
25. Internet Crime Complaint Center, "2021 Elder Fraud State Reports," Federal Bureau of Investigation, 2021.
26. National Council on Aging, "The Top 5 Financial Scams Targeting Older Adults," 27 7 2022. [Online]. Available: https://ncoa.org/article/top-5-financial-scams-targeting-older-adults. [Accessed 8 2 2023].
27. "Keith Darnay," 18 5 2022. [Online]. Available: https://www.kxnet.com/news/top-stories/love-hurts-financially-in-north-dakota-thanks-to-romance-scams/. [Accessed 8 2 2023].
28. K. D. Johnson, "ASU Center for Problem-Oriented Policing," [Online]. Available: https://popcenter.asu.edu/content/financial-crimes-against-elderly-0#:~:text=Many%20elderly%20victims%20do%20not,know%20how%20to%20access%20them.. [Accessed 4 2 2023].

AUTHORS PROFILE

Trang Thi Thu Horn completed her Master's in Cybersecurity and Information Assurance at the University of Central Missouri. She is a member of the Institute of Electrical and Electronics Engineers (IEEE) and the National Society of Leadership and Success (NSLS). Her interested research areas are Cybersecurity and Education.

Dr. Mahmoud Yousef is a professor and graduate coordinator in the Department of Computer Science and Cybersecurity at the University of Central Missouri, Warrensburg, USA. His research area includes Computer Simulation and Modeling, Data Mining, and Computer Science Education. He is a member of the Association for Computing Machinery (ACM), a member of the American Mathematical Society (AMS), and the 2023 conference chair of the Consortium for Computing Sciences in Colleges-Central Plains (CCSC-CP).