International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Comparative Study of Information Security Threats-By Age and Gender

Ms. LAKSHMI K.S [1], Mr. MARIMUTHU R[2]

[1]Ms. LAKSHMI K.S, M.Sc. CFS, Department of Criminology and Forensic Science, lakshmiiyer1399@gmail.com, 9847941790, Dr. MGR UNIVERSITY, Chennai, India
[2]Mr. Marimuthu R, Faculty, Centre for Cyber Forensics and Information Security, University of Madras, Chepauk

---

Abstract - Cybersecurity threats, especially data theft, have become a major concern in today's digital world. As more sensitive information is exchanged online, organizations are at risk of various cybercrimes, such as data breaches, phishing attacks, and ransomware. This study aims to identify and analyze the different threats to information security, focusing on the theft of sensitive data from organizational systems. The main objective of this study is to identify the key information security threats that lead to data theft. To check the authenticity of the website. To analyze how many people have get financial threat.

***Key Words*:** information security, data breaches, security protocols, cyber threats.

1. INTRODUCTION

Information security threats refer to the unauthorized access, disclosure, or destruction of sensitive data, often carried out for malicious purposes. As cyber thefts become increasingly frequent and sophisticated, they pose serious risks to individuals and organizations alike. Cybercriminals leverage methods like hacking, phishing, and malware to exploit vulnerabilities in information systems. This issue is exacerbated by the digital transformation that permeates every aspect of modern life, making it crucial to understand, mitigate, and prevent these evolving threats. This study aims to identify common security threats, analyses their underlying causes and effects, and propose tailored preventive measures.

The theoretical framework of this study is rooted in concepts such as Socio-Technical Systems Theory, which examines how interactions between human and technological elements create security vulnerabilities, and the Human- Behavioral Cybersecurity model emphasizes particular actions which can be influenced by age, gender, and culture. Also, the Risk Perception and Response Framework focuses how differing emotional aspects and perceptions shape cybersecurity responses. These frameworks assist in studying the interference of demographics and behavioral patterns that create vulnerability. The problem under investigation is the unequal distribution of cybersecurity vulnerabilities across demographics. Differences in age and gender significantly shape individuals' digital literacy, online behavior, and susceptibility to cyber threats. Younger gap in perception is caused by younger people being already used to digital environments and therefore taking risks, while older people tend struggling to keep up with the speed of change and becoming more vulnerable. Gender gaps compound risk behavior and threat perception differences since men tend towards engaging in riskier behavior online and women are more often the victims of deceitful phishing campaigns. Most of these aspects are definitely very important, however there is hardly any research exploring the combination of age and gender within the context of information security.

Working on these matters is important not just for the development of the area, but for academic work and practical. Understanding demographic influences on cybersecurity vulnerabilities can enhance individual safety by promoting tailored digital literacy initiatives. Consider designing particular awareness campaigns, training programs, and security measures. Such policies can be crafted to cater to various forms of digital interactions, allowing other scholars to further progress the cybersecurity domain. This study helps to close the gap in age and gender understanding by contributing to the robust and inclusive frameworks for protecting digital assets.

2. LITERATURE REVIEW

LaRose and Kim (2007): LaRose and Young adults aged 18-30 for instance, do tend to recognize new security features, but use them only when it is convenient. As noted by LaRose and Kim. This sets them up to be easily taken advantage of by cyber threats such as ransomware and spyware. The limited cybersecurity risk awareness these young adults pose, makes a strong recommendation for focused cybersecurity education. Underutilized these interventions have the potential to encourage proactive behaviour towards digital safety amongst this

demographic. **Workman (2008):** Women appear to fall victim to more emotionally manipulative scams such as bogus charitable appeals or urgent emergency nudges, while younger men are more likely to be deceived by phishing honey traps marketed using curiosity. These strategies masquerade as rewarding or exclusive content, exploiting specific emotional tendencies. Stereotypical education programs designed to help stronger cybersecurity responders have to be tailored for these distinct gaps in protection. **Prat and Holtfreter (2008)** espouse that elderly women in particular tend to be the target of marketing and email scams because these women are believed to possess funds. These cons perpetrate deceitful claims of favorable finances or urgent appeals, which are hard to detect because they resemble genuine excepted opportunities. There is much to be done, and through targeted instruction, we may offer trustable financial depiction for elderly women to defend themselves against enhanced fraud**. Ng, Kankanhalli, and Xu {2009}** came to a conclusion that women in general are more careful than men when using the Internet in terms of privacy protection. While women take greater care in protecting their privacy, they are also more susceptible than men to phishing scams that invoke fear, urgency, or sympathy. These emotional appeals are specially tailored to make women for such traps. Their strong protective tendency is made ineffective by emotional triggers**. Ngo and Paternoster {2011}** demonstrated that elderly people are the most susceptible audience to phishing and investment scams because of the lack of counter experience. To exploit their ignorance about online security, fraudsters build schemes that seem adequately official. Educating the elderly encourages them to identify these malicious threats protecting themselves in the process**. Furnell and Clarke {2012}** noted that older females, in particular, become more susceptible to online fraud due to lack of confidence with cybersecurity tools. Attackers prey on their emotional and financial vulnerabilities with tactics designed to cultivate fear or sympathy. This increases the likelihood that older women will fall prey to unscrupulous schemes. **Ur et al. (2016):** found that younger people (18-25) often use weak passwords and are more likely to have their credentials stolen. On the other hand, older people tend to create stronger passwords but struggle with managing them securely.

3. PROPOSED METHODOLOGY

The research was conducted using a structured and systematic approach to gather meaningful data related to information security threats. The target population included individuals aged 18 to above 50 years, allowing the study to capture perceptions across different age groups. Before the data collection began, informed consent was obtained from each participant to ensure ethical compliance and transparency. The primary method of data collection was a structured questionnaire, designed to capture information on the types of threats experienced, awareness levels, and responses to such threats. The questions were both close-ended and scaled to support quantitative analysis. After the collection phase, the responses were organized, coded, and prepared for statistical interpretation. The Statistical Package for the Social Sciences (SPSS) software was used for data analysis, allowing the researcher to process large sets of data efficiently and apply descriptive and inferential statistical techniques.

4. RESULTS AND DISCUSSION

Have you or someone you know ever been a victim of online financial fraud or identity theft?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes, I have been affected	25	10.0	10.0	10.0
	Yes, someone I know has been a victim	90	36.0	36.0	46.0
	No, I have not been affected	135	54.0	54.0	100.0
	Total	250	100.0	100.0	

Table 4.1 Experiences with Online Financial Fraud or Identity Theft

The data shows that out of 250 people surveyed, more than half 54% said they have not been affected by online financial fraud or identity theft. The quite of the people 36% reported that someone they know has been a victim of such fraud. Only 10% of the respondents said they had personally experienced online financial fraud or identity theft. This indicates that while direct experiences with online fraud may be relatively low, many people are still indirectly affected through someone they know. Overall, the findings suggest that online financial fraud and identity theft are common concerns, even if not everyone has been personally targeted**.**

How confident are you in your understanding of online security practices (e.g., encryption, secure browsing)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Confident	50	20.0	20.0	20.0
	Somewhat confident	92	36.8	36.8	56.8
	Neutral	83	33.2	33.2	90.0
	Not confident	25	10.0	10.0	100.0
	Total	250	100.0	100.0	

Table 4.2 understanding of online security practices

The survey results show that people's confidence in their understanding of online security practices varies. About 20% of respondents said they feel confident in their knowledge of things like encryption and secure browsing. A larger group, 36.8%, reported feeling somewhat confident, while 33.2% felt neutral—neither confident nor unconfident. Only 10% said they were not confident at all. These findings suggest that while some individuals feel secure in their understanding of online safety, a majority either feel unsure or only somewhat confident, indicating a potential need for more education or awareness around online security practices.

Do you ever share your login credentials (e.g., username and password) with anyone else (e.g., family members, friends)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	52	20.8	20.8	20.8
	No	147	58.8	58.8	79.6
	Sometimes	51	20.4	20.4	100.0
	Total	250	100.0	100.0	

Table 4.3 share your login credentials

The data reveals that most people are cautious about sharing their login credentials. Out of 250 respondents, 58.8% said they do not share their usernames or passwords with anyone. However, 20.8% admitted that they do share their login information, and another 20.4% said they do so sometimes. This means that while a majority avoid sharing their credentials, a significant portion of people still engage in this risky behaviour either regularly or occasionally. These findings highlight the need for more awareness about the potential dangers of sharing login information, even with trusted individuals.

5. ACKNOWLEDGEMENT

I would like to express our sincere gratitude to all those who contributed to the successful completion of this research work. First and foremost, we extend our heartfelt thanks to Dr. M.G.R. Educational and Research Institute, Chennai, for providing us with the necessary infrastructure and academic environment to carry out this project.

I deeply thankful to Mr. Marimuthu.R, Faculty, for his invaluable guidance, continuous support, and insightful feedback throughout the research. His expertise and mentorship were instrumental in shaping the direction and quality of this work.

I also extend our appreciation to our colleagues and peers who provided constructive suggestions and moral support throughout this journey. Special thanks to the faculty of the Department of Criminology and Forensic science for their encouragement and academic assistance.

6. CONCLUSIONS

These study gives an understanding about that the online security remains an important concern for many people. Although 54% of respondents have not been personally affected by online financial fraud or identity theft, 36% know someone who has, and 10% have experienced it themselves. When asked about their understanding of online security practices, only 20% felt confident, while 36.8% were somewhat confident, 33.2% were neutral, and 10% were not confident. Regarding the sharing of login credentials, 58.8% said they never share them, but 20.8% admitted to sharing, and 20.4% said they do so occasionally. These results suggest that while many people take precautions, a large portion still lack strong confidence or engage in risky online behaviour, highlighting the need for more education and awareness around cybersecurity

REFERENCES

1. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.
2. Bishop, M. (2003). *Computer security: Art and science*. Addison-Wesley.
3. Brown, C., & Soni, S. (2019). "Exploring the impact of phishing attacks on organizational security." *Journal of Cybersecurity*, 5(2), 112-130.
4. Casey, E. (2017). *Handbook of computer crime investigation: Digital forensics and cybercrime*. Academic Press.
5. Cisco Systems. (2020). "2020 Annual cybersecurity report." Retrieved from https://www.cisco.com
6. European Union Agency for Cybersecurity (ENISA). (2020). "Cybersecurity threats and trends: 2020." Retrieved from https://www.enisa.europa.eu
7. Greer, K., & Venkatesh, V. (2020). "Impact of human behavior on cybersecurity vulnerabilities." *International Journal of Information Security*, 13(4), 89-105.
8. Hu, Q., & Xu, J. (2018). "A survey on information security threats in cloud computing environments." *Journal of Cloud Computing: Advances, Systems, and Applications*, 7(1), 1-
9. NIST. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology.
10. Reeder, J., & Desai, M. (2017). "The rise of ransomware: Understanding the security risks and mitigation strategies." *Cybersecurity Review*, 4(3), 45-60.
11. Risk Based Security. (2019). "2019 Data Breach QuickView." Retrieved from https://www.riskbasedsecurity.com
12. Schneier, B. (2018). *Secrets and lies: Digital security in a networked world*. Wiley.
13. Smith, A., & Wilson, M. (2017). "Cybersecurity threats in the financial sector." *Journal of Financial Security*, 12(3), 211-230.
14. SANS Institute. (2021). "Top 20 critical security controls." Retrieved from https://www.sans.org
15. Symantec Corporation. (2020). "Internet security threat report: 2020." Retrieved from https://www.symantec.com
16. Verizon. (2020). "2020 Data breach investigations report." Retrieved from https://www.verizon.com
17. Westin, A. F. (2017). *Privacy and freedom*. Ig Publishing.
18. Wheeler, D. A. (2021). "Security threats in the digital age: A focus on emerging technologies." *Journal of Technology and Cybersecurity*, 9(2), 32-48.
19. Zetter, K. (2019). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown Publishing.
20. Zhang, L., & Wu, M. (2020). "A study of advanced persistent threats (APT) in information security." *Journal of Cybersecurity and Information Management*, 8(4), 200-215.