International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

ANALYSIS OF PROTECTING DIGITAL ASSETS AMONG MILLENNIALS

DR. UMAKANTH.S[1], TANVI SIOTIA[2], ARYAN GUPTA[3], RISHABH KUKHRANIA[4], TANISHI GUPTA[5], SHARANASH BHILWARIA[6], MINDAKUDURU BHANU MURTHY [7]

[1] Prof & HOD JAIN (DEEMED TO BE UNIVERSITY)- CMS
[2] STUDENT BBA, CENTER FOR MANAGEMENT STUDIES, JAIN(DEEMED TO BE UNIVERSITY)
[3] STUDENT BBA, CENTER FOR MANAGEMENT STUDIES, JAIN(DEEMED TO BE UNIVERSITY)
[4] STUDENT BBA, CENTER FOR MANAGEMENT STUDIES, JAIN(DEEMED TO BE UNIVERSITY)
[5] STUDENT BBA, CENTER FOR MANAGEMENT STUDIES, JAIN(DEEMED TO BE UNIVERSITY)
[6] STUDENT BBA, CENTER FOR MANAGEMENT STUDIES, JAIN(DEEMED TO BE UNIVERSITY)
[7] STUDENT BBA, CENTER FOR MANAGEMENT STUDIES, JAIN(DEEMED TO BE UNIVERSITY)

DOI : https://doi.org/10.5281/zenodo.15101230

ABSTRACT -

This investigation explores the challenges millennials face in safeguarding their digital assets in an era of rising online fraud. Due to their heavy reliance on technology, the millennials are bound to be vulnerable to cybercriminals. The study examines key risk factors, including their dependence on digital platforms, lack of cybersecurity expertise, and overconfidence in their knowledge. It also highlights common types of online fraud targeting millennials, such as phishing, investment scams, social engineering, and identity theft. Findings show that 50% of millennials have experienced some form of online fraud, yet only 35% regularly use strong passwords or two-factor authentication. Furthermore, cybercrime targeting millennials has increased by 30% over the past five years, underscoring their growing exposure to these threats. The study also highlights the importance of millennials adopting a more proactive stance toward cybersecurity by increasing awareness of potential risks and promoting safer online practices. It suggests that using password managers can help securely store and organize login information, decreasing the chances of using weak or repeated passwords. Additionally, the study recommends that tech companies and educational institutions collaborate to offer resources and training that equip millennials with the necessary tools and knowledge to protect their digital assets. Given their increasing reliance on digital services, it is essential for millennials to prioritize online security in order to reduce the growing threat of cybercrime. The study concludes with recommendations for improving cybersecurity practices, such as creating strong passwords, enabling two-factor authentication, and staying updated on security developments.

Key words : Digital age , technological enhancement, cyber fraud , millennials , phishing , malware, assets , cyberspace.

1. Introduction -

Digital age has modified all levels of life by offering unlimited information, interaction, language to use and work to perform. Nevertheless, technological enhancement continues to create more risks in society, most especially for digital gadgets. Cyber fraud is a global menace and risks inflicted to individual and corporate entities. Due to their excessive online interactions and infatuation with digital media, the most internet society, the millennials, are mostly affected by such crimes. Thesis statement of the paper is articulated in regards to solutions that will assess the extent of destruction posed on these groups and minimize these threats further enhancing the cyber safety of millennials.Security education. Most of the millennials belong to the technology generation where they have grown up with technology from a young age. Nevertheless, being advanced in using devices does not equate to mastery of the concepts and the practices pertaining to the security of information and networks. These overestimations and advanced technicalities thus put the people in danger of being preyed upon by phishing and other malwares. This overconfidence can result in a self-defeating measure of protection thus making them targets for social engineering. To illustrate, individuals within the millennial generation may be gullible enough to open mail from strangers or even hyperlinks and download materials assuring themselves that they are able to spy and detect the bad stuff. Crime. Having the ability to control one's finances, use the services of other people, and perform business transactions through the internet is quite pleasant. Still, these conveniences can pose threats to unsuspecting users as there are unscrupulous people who tend to take advantage of them. In this regard, it has been found that millennials do not shy away from using public WIFI networks or even interacting with random people over the internet, both of which are risky behaviours. In order to achieve such a goal: There is a need to formulate implementation strategies, health education plans and develop appropriate measures. These programs should aim at educating the people about the perils of cyber networks; practical tips on how one can keep his/her gadgets safe from such threats and promoting appropriate use of the internet. Optimism with which they regard the digital environment ought to be tempered with a healthy sense of caution and a readiness to guard against possible threats to their safety. In their case however, fraud has morphed in a different way: New technologies have changed almost every sphere of their lives for the better. Nevertheless, there are new drawbacks accompanying them- in particular the challenge of online scams. This is in view of cybercriminals and the unique characteristics of millennials. In doing so, we can design ways of helping them guard their assets in the cyber world against threats and stay out of the dangers posed by cyberspace.

2. Review of literature -

1. **Millennials and Cybersecurity: Habits, Concerns, and Solutions," Rainie, L., and Anderson, J. (2020).** The Pew Study Centre. This study examines the cybersecurity behaviours, concerns over internet safety, and self-defence tactics among millennials. It illustrates how millennials are vulnerable to cyberattacks because, despite their technological prowess, they usually overlook the gravity of some online threats.

2. **Digital Literacy and the Protection of Digital Assets Among Millennials: A Growing Concern," Gupta, A., and V. Jain (2020).** Journal of Information Security. This study discusses the significance of digital literacy for the preservation of millennials' digital assets. It emphasizes how important knowledge is to using online platforms safely.

3. **Martin, C. P. and Zhou, X. (2021). Cybersecurity review titled"Millennials and the Difficulties of Protecting Private Digital Data:** A Changing Environment. This review addresses the evolving nature of cybersecurity risks and how millennials protect their personal digital information.

4. **Kim, S. and Kang, T., "The Impact of Cybercrime on Millennials' Digital Asset Management," (2021).** Journal of Financial Crime.This study looks into how millennials handle digital assets and the rise in cybercrime. It considers personal and financial assets that are stored online.

5. **Adopters: Millennials tend to overlook these risks. Implementing enhanced financial security protocols and user education is recommended. Varma, S., and R. Ghosh (2021).** "A Systematic Review of Millennials' Digital Asset Security Behaviours." Journal of International Cyber Studies.

6. **In 2022, Williams, M., and Patel, D. "Millennials and Online Fraud:** Preventive Steps and Knowledge." Journal of Financial Services and Technology. This study looks at how online fraud is increasingly targeting millennials and assesses their familiarity with fraud prevention tools.

7. **Chaudhuri, A., and S. Bose. "Online Financial Fraud and Millennials: A Behavioural Approach to Protection." (2022).** The Finance Journal's Consumer Research. This essay uses a behavioural approach to explain why millennials are susceptible to online financial fraud and what can be done to protect them.

8. **"Millennials' Digital Asset Management: The Significance of Fintech Security." Ali, N., and Khan, M. (2022).** International Journal of Finance and Cybersecurity. This paper examines the widespread use of fintech services by millennials.

9. **Smith, H., and Muller, R. (2022).** "A Survey Based Approach to Assessing Millennials' Knowledge of Digital Privacy Tools." Information Security Journal. This study assesses millennials' knowledge of privacy tools, such as virtual private networks (VPNs) and encrypted messaging, and how to utilize them to protect digital assets.

10. **"A Comparative Analysis of Millennials' and Older Generations' Awareness of Digital Security." Choi, J., & Park, M. (2023).** Journal of Digital Security. This study looks at the differences between millennials and previous generations. in their knowledge of and commitment to online safety.

3. Statement of the problem -

With the upward push of digital platforms, Millennials face increasing risks of cyber threats, records breaches, and identification theft. As a generation deeply included with the era, they regularly prioritize convenience over safety, leaving their digital assets prone. Despite existing recognition efforts, many nevertheless lack proper information about cybersecurity nice practices. This takes a look at examines Millennials’ virtual security habits, the effectiveness of current protective measures, and methods to promote moral and sensible cybersecurity practices. The research paper aims to analyze & understand the risk involved with millennials in protecting digital assets & virtual behavior of millennials.

4. Objectives of the study-

a) To analyze the millennials understanding of digital asset & online fraud

b) To find the millennials digital securities practices during online activity
c) To understand the cyber security awareness among the millennials
d) To find the online transaction practice among the millennials
e) To analyze the cybersecurity consciousness among millennials

5. Scope of the study-

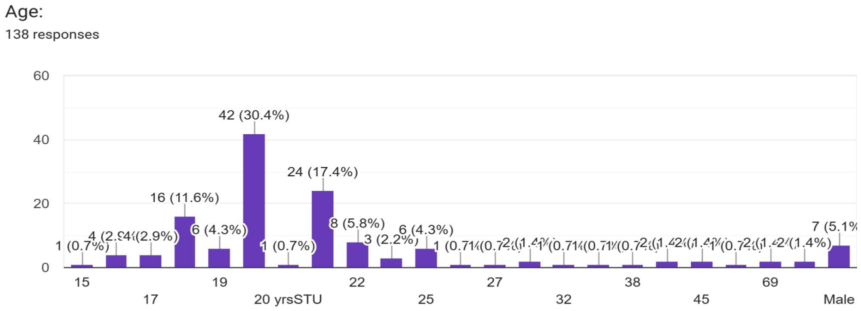
The analysis of Protecting Digital Assets Among Millennials can focus on the following aspects: Comprehension of Digital Assets - Elucidation along with classifications of digital assets such as personal data, cryptocurrency, digital identities, and intellectual property, among others.
What role does digital assets play in day-to-day living? Ownage of Digital Assets Amongst Millennial - Digital assets that millennials most commonly possess. The interaction of millennials with digital assets. Perceptions and knowledge regarding the safeguarding of digital assets. Cybersecurity Knowledge of Millennials - Cyber threats understanding (hacking phishing, identity theft, ransomware, etc.) Known practices for the best protection of digital assets. Protected youth; knowledge deficiency areas in cybersecurity. Techniques of Safeguarding Digital Assets - Hashing, 2FA, strong passwords, and other encryption techniques. Digital wallets and other secure storage practices. Legal and moral concerns regarding the protection of digital assets. This research shows the Digital Security Problems of Millennials -Malpractices in protecting digital assets and common security shortcomings. Security neutral behavior tendencies.The role of social media and excessive sharing. Impact of Technology and Digital Tools

6. Methodology-

This study adopts a mixed-methods research design, combining both qualitative and quantitative approaches to gain a comprehensive understanding of how millennials protect their digital assets, their cybersecurity behaviors, and the risks they face.The research is designed as an exploratory study that investigates the cybersecurity practices of millennials and their vulnerabilities to digital threats. The study focuses on key areas such as cybersecurity knowledge, digital asset management, fraud risk exposure, financial technology risks, and social media privacy concerns.Data Collection The study employs multiple data collection techniques to ensure a well-rounded analysis: Surveys & Questionnaires Purpose: To gather large-scale, quantitative data on millennials' knowledge, attitudes, and behaviors regarding digital security. Instrument: A structured questionnaire developed using Google Forms or other survey tools(e.g.,SurveyMonkey, Qualtrics). Sample Size & Distribution: Responses are collected from a diverse group of millennials, including students, professionals, and entrepreneurs. Key Topics Covered:Awareness of cybersecurity risks (e.g., phishing, identity theft, data breaches).

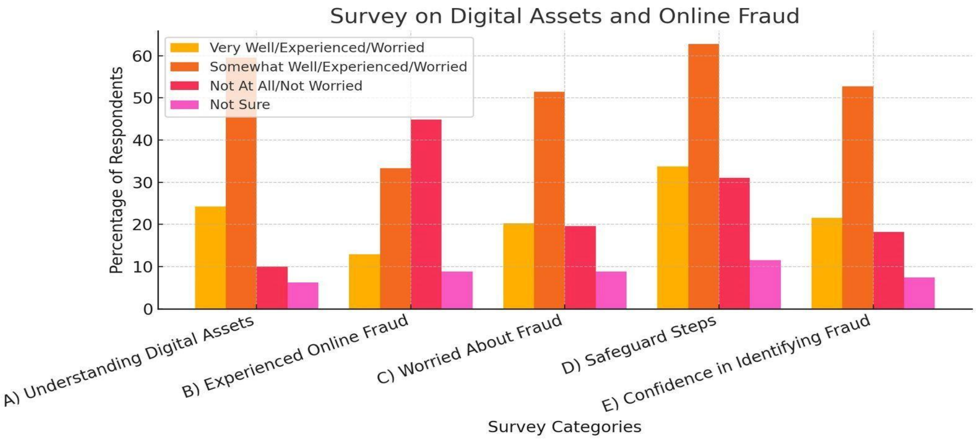
7.Data analysis and interpretation :

Chart-1 Showing the age of respondents



Analysis Interpretation
The bar chart represents the age distribution of 138 respondents. Most of the participants fall in the younger demographic, with 42 respondents (30.four%) aged 19 being the most represented. That is followed by 24 respondents (17.four%) elderly 20, and 16 respondents (11.6%) elderly 18. There are scattered responses from members elderly 27, 32, 38, 45, and 69, each constituting less than 1.

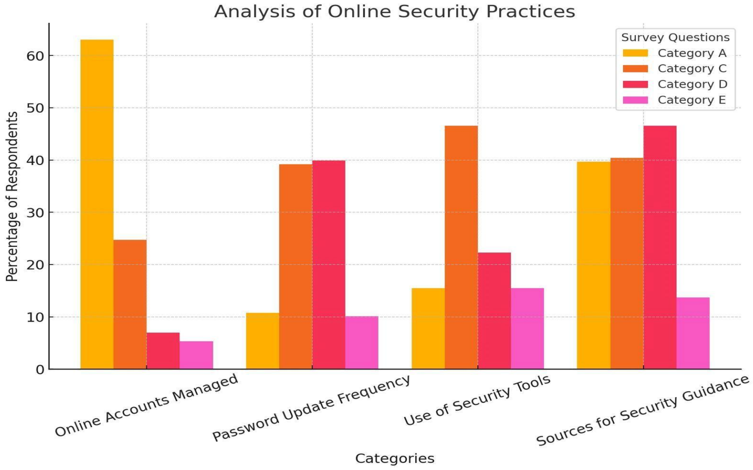
Chart-2 Showing the respondents understanding & experience of digital asset & online fraud



Analysis Interpretation

The research findings reveal key insights into millennials' understanding, experience, concerns, and security measures regarding digital assets. A majority (59.5%) of respondents have a somewhat understanding of digital assets, while only 24.3% claim to understand them very well, indicating a knowledge gap in this area. When it comes to online fraud, 12.9% of respondents have personally experienced it, while 33.3% know someone who has been a victim, highlighting the prevalence of cyber threats

Chart-3 Showing the digital security practices of digital asset and online fraud

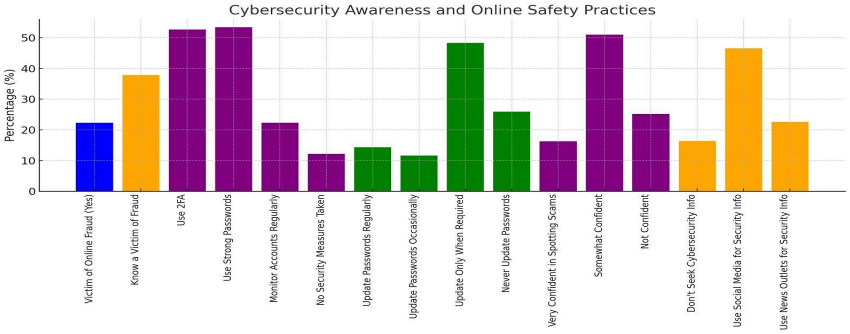


Analysis Interpretation

The data reveals important insights into millennials' digital security habits. The majority of respondents (63%) manage between 1-3 online accounts, while 24.7% handle 4-6 accounts, indicating significant online activity. However, password management practices appear inconsistent, with only 10.8% updating passwords monthly, while 39.2% do so every few months and another 39.9% rarely update them.

Chart-4

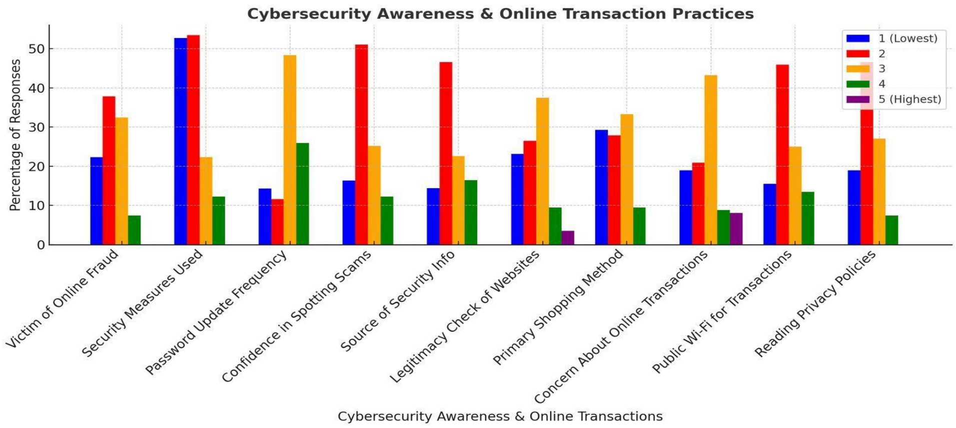
Showing Cybersecurity Awareness and Online Safety Practices of digital asset and online fraud



Analysis Interpretation

The analysis highlights cybersecurity consciousness gaps. whilst 22.three% have confronted on-line fraud and 37.eight% recognise victims, security measures are inconsistent. Even though fifty two.7% use 2FA and fifty three.4% depend upon strong passwords, most effective 22.3% monitor debts, and 12.2% take no precautions.

Chart-5 Showing Online Transaction Practices of digital asset and online fraud



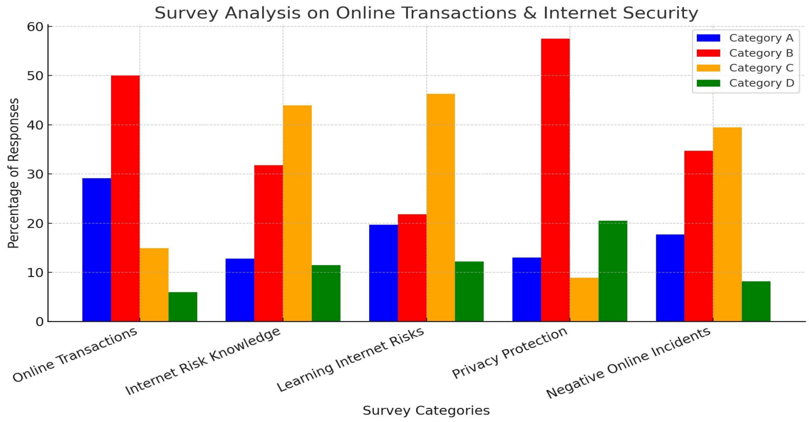
Analysis Interpretation

The evaluation reveals gaps in cybersecurity focus. Even as 22.3% have faced online fraud and 37.eight% know a victim, protection practices are inconsistent. 52.7% use 2FA and fifty three.4% depend on sturdy passwords, handiest 22.three% screen bills, and 12.2% take no precautions. Password updates are infrequent, with 48.3% updating handiest while wanted and 25.nine% never. self belief in recognizing phishing scams is moderate, with 51% truly confident and 25.2% not confident at all.

Chart- 6

Showing Cybersecurity consciousness and online privacy behavior

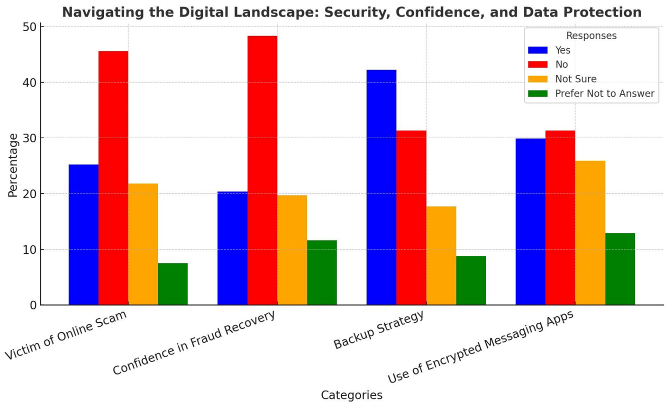
of digital asset and online fraud



Analysis Interpretation

The survey highlights combined awareness of cybersecurity risks. At the same time as 50% occasionally and 29.1% regularly behave online transactions, forty three.9% price their net risk information as low, and simplest eleven.5% recall themselves professionals. maximum (46.3%) study via films, while fewer depend upon blogs (19.7%) or webinars (21.8%).

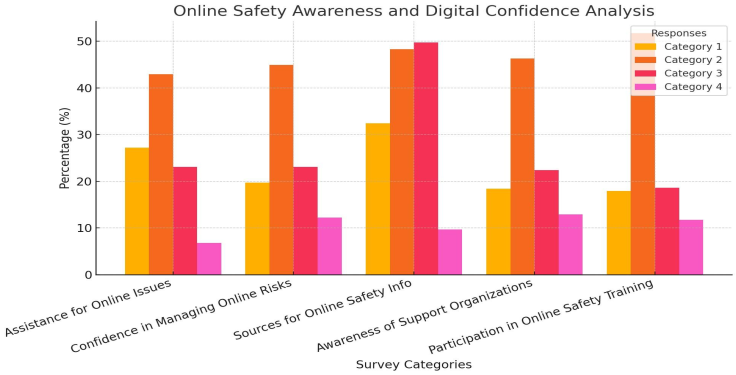
Chart-7 Showing navigation of the digital landscape : security , confidence, and data protection



Analysis Interpretation

The information highlights online safety behavior and virtual safety. whilst 45.6% have in no way fallen for scams, 25.2% have, displaying ongoing cyber risks. Self assurance in fraud healing is low, with 48.three% feeling unprepared.

Chart-8 Showing digital literacy and online safety awareness of digital asset and online fraud



Analysis Interpretation

The survey well-known shows gaps in digital literacy, with forty two.nine% blind to wherein to searching for assistance and forty four.9% only incredibly confident in handling on-line dangers. most rely on friends (49.7%) and social media (48.3%) for online protection data rather than authentic resources.

8. Results and findings-

The results & findings across various studies in the provided literature reveal several key insights into the challenges millennials face in protecting their digital assets, as well as the solutions proposed to mitigate these risks. Here's a summary of the findings:

1. 1)**Vulnerability Due to Overconfidence**: Millennials, despite being tech-savvy, tend to overestimate their ability to manage cybersecurity risks. This leads to risky behaviors like not using strong passwords, neglecting to enable two-factor authentication, or falling for phishing attempts Cybersecurity Knowledge.Many millennials lack basic cybersecurity knowledge, despite their extensive use of digital services. Studies have shown that while they use digital platforms extensively, they often overlook essential security measures .

2. 2)**Risks from Online Fraud**: Increasingly targeted by online fraud, including phishing, identity theft, social engineering, and new forms of fraud like deep fake attacks . Their reliance on public Wi-Fi networks and engageases their susceptibility to these threats .

3. 3)**Digital Asset Management**: Millennials are managing significant personal and financial information online but often fail to follow appropriate security protocols. This lack of attention to digital asset security makes them vulnerable to cybercrime .

4. 4)**Cybersecurity Solutions** : A recurring recommendation across studies is education for millennials. This includes incorporating cybersecurity topics into curricula and workplace training to raise awareness of potential risk .The studies emphasize the importance of easy-to-use security tools, such as password managers and millennials taking action without feeling overwhelmed .

5. 5)**Financial Technology and Cryptocurrency Risks** : - The growing use of financial technologies and cryptocurrencies among a set of challenges, as they often lack knowledge about the security risks associated with these platforms .

6. **Privacy Concerns in Social Media**: - Millennials' heavy use of social media platforms increases the risks of data breaches and online fraud. Sharing information online makes them vulnerable to identity theft and other forms of exploitation .

7. **Behavioral Factors** :- Behavioral factors, such as a preference for convenience over security and a tendency to trust online interactions too easily, contribute to to cyber threats

9. Suggestions and recommendations :

Based on the findings of this study, the following recommendations aim to enhance millennials' cybersecurity awareness, protect their digital assets and minimize their vulnerability to online fraud.

- **Mandatory Two-Factor Authentication (2FA):** Online platforms, especially in banking, e-commerce, and social media, should enforce 2FA to enhance account security.
- **Adoption of Password Managers:** Individuals should use password managers to generate and store unique, strong passwords for multiple accounts. Users should be reminded to update their devices and applications frequently to protect against security vulnerabilities.
- **Reducing Risks in Financial Technology and Cryptocurrency**

- **User-Friendly Security Features:** Financial technology platforms should integrate security guidelines, fraud alerts, and transaction verification steps to protect users.
- **Verifying Financial Platforms:** Millennials should be educated on how to identify legitimate financial services, verify regulatory compliance, and avoid fraudulent investment schemes.
- **Safe Online Transactions:** Users should opt for secure payment gateways, virtual credit cards, and fraud alerts to minimize risks when making online purchases.
- **Conclusion:** By adopting these recommendations, millennials can better protect their digital assets, minimize cyber risks, and establish a more secure online presence. Increasing cybersecurity awareness, implementing practical security measures, and promoting a proactive approach to digital safety will be essential in reducing vulnerabilities and mitigating future threats.

10. Conclusions -

To summarize, the unique challenges of safeguarding digital assets portray youth's relationship with technologyTherefore, safeguarding their digital assets is critical, but they often fail to take adequate protective measures. Millennials, in comparison to older generations, are more aware of cybersecurity risks, especially those related to hacking, phishing, and data leaks.However, proactive, long-term steps are not necessarily a direct outcome of this awareness. Even as they realize how much it matters, many millennials rarely update security software, use strong passwords, or employ two-factor authentication. The biggest challenge of this age is finding a balance between security and usability, as most digital solutions prefer user-friendliness over robust security. To solve these problems, better cybersecurity technologies and specialized education must be considered with the requirements and digital habits of millennials.Beside creating awareness, the educational initiatives should focus on bridging the knowledge gap and focusing on actionable steps that millennials can take to ensure their digital assets.

11. REFERENCES-

1. Lusardi, A. (2019). Financial well-being of the Millennial generation: An in-depth analysis of its drivers and implications. *Global Financial Literacy Excellence Center*, 1-7.
2. Munadiati, M., Kurlillah, A., Iskandar, I., & Hamid, A. (2022). Risk Management Analysis and
Profit Maximization of Indonesian Millennials Investing in Cryptocurrencies. *Al-Muamalat: Jurnal Hukum dan Ekonomi Syariah*, *7*(1), 13-30.
Herrera, I. M., & Caballero, M. G. (2024). MILLENNIALS AND GENERATION X FACING THE
3. REALITY OF BIG DATA AND THE PROTECTION OF PERSONAL DATA ON THE INTERNET.
Vivat Academia, (157), 1-18.
4. Jahankhani, H., Kendzierskyj, S., & Popescu, I. O. (2023). Millennials vs. Cyborgs and Blockchain Role in Trust and Privacy. In *Research Anthology on Convergence of Blockchain, Internet of Things, and Security* (pp. 1167-1192). IGI Global.
5. Rahayu, R., Ali, S., Aulia, A., & Hidayah, R. (2022). The current digital financial literacy and financial behavior in the Indonesian millennial generation. *Journal of Accounting and Investment*, *23*(1), 78-94.
6. Dash, G., Kiefer, K., & Paul, J. (2021). Marketing-to-Millennials: Marketing 4.0, customer satisfaction and purchase intention. *Journal of business research*, *122*, 608-620.
7. Putri, R. A., & Tri Putrajaya, A. I. (2024). Analysis of the Influence of the Use of Fintech Services on Investment Decisions of Millennial Communities in the Digital Age. *Journal of Social Science*, *5*(6), 1501-1512.
8. Sharmin, F., Sultan, M. T., Badulescu, A., Bac, D. P., & Li, B. (2020). Millennial tourists' environmentally sustainable behavior towards a natural protected area: An integrative framework. *Sustainability*, *12*(20), 8545.
9. Divekar, B. D. R. (2025). A STITCH IN TIME: A Study on the Latent Factors of Awareness and Perception of Sustainable Estate Planning Among Millennials in Urban Bengaluru. *Securing the Future through Sustainability, Health, Education, and Technology*, 164.
10. Abdillah, A., Basuki, H., Santoso, W. I., Sukresna, I. M., & Indriani, F. (2024). Utilization of Digital Banking Services for Generation Z Economic Sustainability. *Research Horizon*, *4*(4), 11-22.
11. Murphy, H., Keahey, L., Bennett, E., Drake, A., Brooks, S. K., & Rubin, G. J. (2021). Millennial attitudes towards sharing mobile phone location data with health agencies: a qualitative study. *Information, Communication & Society*, *24*(15), 2244-2257.
12. Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5*, 100165.
13. Zitha, T., & Penceliah, D. (2022). Perceptions regarding digital payments in online shopping amongst millennials in KwaZulu-Natal, South Africa. *African Journal of Inter/Multidisciplinary Studies*, *4*(1), 338-349.
14. Handayani, I., & Agustina, R. (2022). Starting a digital business: Being a millennial entrepreneur innovating. *Startupreneur Business Digital (SABDA Journal)*, *1*(2), 126-133.
15. Qureshi, M. A., Khaskheli, A., Qureshi, J. A., Raza, S. A., & Khan, K. A. (2023). Factors influencing green purchase behavior among millennials: the moderating role of religious values. *Journal of Islamic Marketing*, *14*(6), 1417-1437.