Int. J. Sci. R. Tech., 2026 3(3)
A Multidisciplinary peer-reviewed Journal
www.ijsrtjournal.com [ISSN: 2394-7063]

Original Article

Cyber Security Awareness Among Genz

J. Anurushmitha*[1], D. Nikhitha[2], J. P. Pramod[2]

[1]*B. E Student, Department of Electronic and Communication Engineering, Stanley College of Engineering & Technology for Women, Abids, Hyderabad, Telangana, India*
[2]*Assistant Professor, Department of Physics, Stanley College of Engineering & Technology for Women, Abids, Hyderabad, Telangana, India*

ABSTRACT

This paper investigates the extent to which Generation Z has an understanding and awareness of cyber security and its threats. Generation Z is defined as people about 15 to 25 years old (as of 2025). They have lived through extraordinary technological advancement with digital devices, smart applications, social media, and online learning environments becoming a part of their daily lives. Generation Z's extensive use of digital technologies for their education, entertainment, social interaction, and work has created an interconnected individual but also heightened vulnerability to cyber threats. The opportunity for significant change in the digital creation will only continue to increase the significance of teaching and building a strong cyber security awareness among this cohort. Cyber security awareness is the knowledge and understanding that is necessary for the identification of potential cyber threats and taking steps to use safe practices to prevent compromise of your data, privacy, and digital identity. For Generation Z, who often spend a lot of time online, their awareness of potential cyber threats is a critical part of minimizing exposure to a variety of risks, such as phishing, hacking, data breaches, identity theft, cyberbullying, and/or online scams. The fact that Generation Z is generally willing to share information about themselves, to engage on multiple digital platforms, is a potentially dangerous vulnerability - usually exposing them even more to malicious attacks. Learning early about cyber security practices that lead towards building safe online habits should be an important part of cyber safety education, as children will bring these safe practices into adulthood. The text addresses that while most of Generation Z understands basic risks associated with online tools, they may misjudge the extent to which modern cyber-Attacks are organized, relentless, and adaptive. Generation Z also tends to be highly reliant upon technology without basic critical thinking or digital literacy skills effectively to assess some risks. The speedy nature of social media platforms, online gaming, and source of digital communication create blurred lines between public and private spaces, and make younger users more vulnerable to manipulation, misinformation, and fraud. If we could strengthen cyber security education, Generation Z may be better able to defend themselves and others in cyberspace, and become better citizens and workers. Creating cyber security awareness is a teamwork approach involving educational institutions, governments, families, and technology companies. School systems and universities can demonstrate their commitment to cyber security education by including it in their curriculam. Through curriculum, classroom activities, school creations - giving students meaningful experience of creating strong passwords, identifying potentially malicious phishing emails, managing their digital footprints, privacy settings - schools can practice and experience cyber security. Awareness campaigns, workshops, and simulations are also very useful to train Generation Z in practicing safe online behaviors and the potential real-world implications of a Cyber Attack. Further, parents and caregivers also play an important role in bringing behavioral awareness to the family and allowed to model responsible online behavior, and promotes open discussions about digital safety.

Keywords: cyber risks, cyber security, cyber threats, online bullying, psycho social

INTRODUCTION

Cyber security is the art and science of securing our digital lives. The term describes all protections in digital spaces, along with protections for our accounts, passwords, photos, and scams. Cyber security should be considered sometimes like a shield to protect the online world. Cyber security, related to monitoring, detects fake links. The following discussion relates to how Gen Z is interfacing with cyber security. Generation Z is the word used to refer to people between the ages of 15 & 25 in the year

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

2025. This generation grew up with digital technology, including smart technology, social media, and online learning platforms that are fully integrated into their daily life on the Internet. Another way to think about these young people is that they exhibit qualities of acting quickly, decreasing social interactions, little self-discipline, and found tempted to something with little awareness of consequences of use. Next to Millennials (who are between ages 30 – 40), Gen Z grew up during the digital present, are truly tech natives, and will have spent a substantial amount of time online, compared to Millennials, with a great deal of time spent on sharing their daily activities, reels, photos, locations, and videos. Therefore, Gen Z is subjected to substantial cyber risks. While Millennials are balancing their digital life by being conscious of privacy, Gen Z tends to gravitate toward platforms such as Tik Tok, Instagram Reels, Snapchat, memes, and newer trends. Millennials tend to be more active on Facebook, Twitter, and like to have detailed posts. Gen Z is very active in social media while the Millennials tend to be more conservative. Gen Z uses social media platforms to express themselves. The viral trends encourage them to be revealing and share private information. By sharing their information, scammers or hackers can quickly gain access to their information and utilize it through exploiting them. This understanding empowers Gen Z and decreases the likelihood of privacy breaches, minimalizing risks and threats, and privacy theft, and they still implement technology. Although Gen Z are adept at using technology online, many do not have solid understanding of cyber security awareness or the potential consequences of their online behavior. Essentially, because Gen Z have spent so much time on their devices, and because there is a growing expectation that the online environment should have an element of normalcy, Gen Z has developed a …sense of security that is not assessed, justified, warranted, or promised at all. Most either do not see a need for precautions or have not thought about how easy it is to misuse any type of data once it is uploaded or shared online. As cyber threats (such as phishing, identity theft, malware, fake websites and social engineering) become more advanced and are emerging more brazenly, this group becomes more vulnerable and exposed. In addition, peer pressure (including someone, beside a close friend, becoming popular very quickly online) causes Gen Z to ignore or disregard privacy settings, and to read security advisories or warnings, as just a normal part of their instruction. Another issue is - the minimal role of schools and colleges in cyber security awareness. This generation has relatively strong technical literacy skills but usually it is situational usage knowledge. Gen Z may be proficient at navigating apps, but that knowledge does not coalesce to include more complex, system-level, security terms - that often accompany technology programs. Educational community members, parents, and government entities should be mindful of their responsibility to promote safe online practices. By embedding cyber security within the educational curriculum, educating the public via awareness campaigns, prompting awareness of digital behaviors, etc., we can help combat the issues we face in online experiences. Educational forums, engage learning, or practical examples can be illustrative to demonstrate how a simple action, such as clicking on a nefarious hyperlink or sharing a password, can lead to tragic outcomes. Furniture of cyber security awareness is paramount in order to cultivate good online practices among Gen Z. Educating this generation with their Equippable knowledge will assist them in becoming a first line of defense against cyber ecosystems. A secure digital future is not only technological, but lies in the hands of credible users who appreciate the significance of privacy and the obliteration of data to keep them safe.

LITERATURE REVIEW:

In recent years, cyber security awareness has become an important area of research as the digitalization continues to reshape how people live, learn, and communicate. Cyber security awareness, as it relates to the individual, is the ability to recognize potential cyber threats, understand how to respond, and take precautionary steps to protect self-information and activities online. As cybercrimes targeting young users continued to emerge, along with an increase in phishing attacks and identity theft cases, more researchers began targeting Generation Z, the first generation to be completely immersed in the digital age. While members of Generation Z are known to be highly connected digital users, this also comes with advantages and disadvantages for cyber security. While some studies have shown that Generation Z has high digital literacy, some studies have shown a lower

awareness of cyber security. Hadlington (2017) noted that younger users often do not view themselves as susceptible to online threats yet exhibit proficiency in using digital tools. Younger generations may not understand other forms of online threats, objects that would inherently compel caution. In a different study, Ng, Mc Coombe, and Wong (2020) noted that young individuals have the tendency to be overconfident in their ability to manage digital risk, as they engage in careless behaviors within the digital environment, which include: reusing passwords; ignoring privacy settings; and downloading unverified applications, or incompatible apps. Alotaibi's (2021) study recommended that university students—young individuals who often engage with the most online—often fail to discern. Research papers already conducted demonstrate a full understanding of Generation Z's challenges with cyber security and levels of awareness. Most studies suggest education and training critically impacts an individual's ability to practice safe online behaviors. Research has shown that interactive awareness programs, game learning tools, and workshops can lead to substantial improvements in user awareness (Kaur & Singh, 2020). Unfortunately, a disconnect between understanding and credentials remains evident, as many can identify and articulate risk without exhibiting any secure practices in their day-to-day lives Some studies view a focus on the 'privacy paradox'—in which Generation Z expresses concern about privacy issues but still publicly shares their data on social media (Baruh et al., 2017). Other research discusses geographic differences, as adolescents in developed countries typically demonstrate greater access to education in cyber security compared to their peers in developing regions, thereby exacerbating ignorance in practice. More recent studies continue to look at the influence of artificial intelligence, phishing, and deep fake technologies on Generation Z's anxiety about cyber threats.

METHODOLOGY:

Cyber security awareness refers to an understanding of online risks and appropriate responses to protect personal and digital data. A high proportion of Generation Z age group is now online, including through social media, gaming, and cloud-based platforms, and therefore awareness is especially relevant. Generation Z is generally "digital natives" and is very familiar with working with technology; however, specifically many in this cohort may not have had sufficient exposure to the advanced online threats and risks such as phishing, malware, ransom ware, and data breaches. Habitual risky or impulsive behavior, and convenience, can put this generation at higher risk while online to provide personal and digital information.

Technological Skills: An assumption and belief that one has organizationally competent technical skills can lead to careless online activity surrounding protection.

Absence of Formal Education: Educational institutions may be teaching digital literacy skills, but most likely are not teaching privacy, ethics, and in general, cyber protection behaviors.

Social Media: The desire for likes and followers (the use of social media) leads to over sharing.

Peer Pressure and Trends: Someone could be tempted to participate in a viral social media challenge that did not use sound judgment.

Limited awareness campaigns: Some of the younger user community is simply unaware of organizations that promote youth focused cyber-awareness initiatives.

- **Common Cyber security Threats**

Phishing: A phishing scheme uses some misleading messages to obtain an individual's personal identifiable information (PII).

Fraud and Scams on Social Media: Users may be contacted by fake social media accounts or offering a giveaway or stock investments to finance, or obtain users' money, or obtain access to users' personal identifiable information (PII).

Identity Theft: Some individuals may over share personal identifiable information (PII) about themselves, making it easy for the cybercriminals to misuse this information.

Malware and Ransom ware: malware, including ransom ware can hijack an individual's device, data, or sensitive information.

Cyberbullying and Harassment: Harassment can start on social media or another publicly available site.

Data Breaches: An individual could be impacted by a data breach on a third-party website which the user may use in some type of paid/subscription capacity. This study utilizes a mixed-method approach to understand directorate cyber security awareness for Generation Z (Gen Z) by combining three complementary sources of information: a structured online survey, online behavior data analysis and literature review of recent reports. This integrated approach allows for a comprehensive understanding of how Gen Z understands, acts and experiences cyber security in the digital sphere.

- **Survey with Gen Z**

To understand levels of awareness, behavior practices and experiences around cyber threats, a survey of 500 Gen Z respondents (15-26 years old) was administered online. The survey was circulated through University networks, social media in groups and on apps such as Instagram, WhatsApp and Telegram. Convenience sampling was stratified to identify gender, age group and education balance. The survey included both closed and open-ended questions, and was designed to measure knowledge, attitudes and behavior with respect to cyber security. Sections to the survey included demographics, social media use, awareness of online threats and countermeasures, and prior experiences of cyber trauma. Survey questions were well-considered relative to standard cyber security awareness models. A pilot study was also used to test the survey for clarity and reliability with 30 respondents.

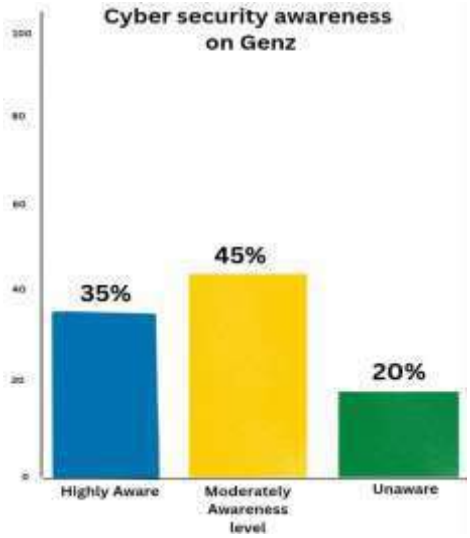

Figure 1

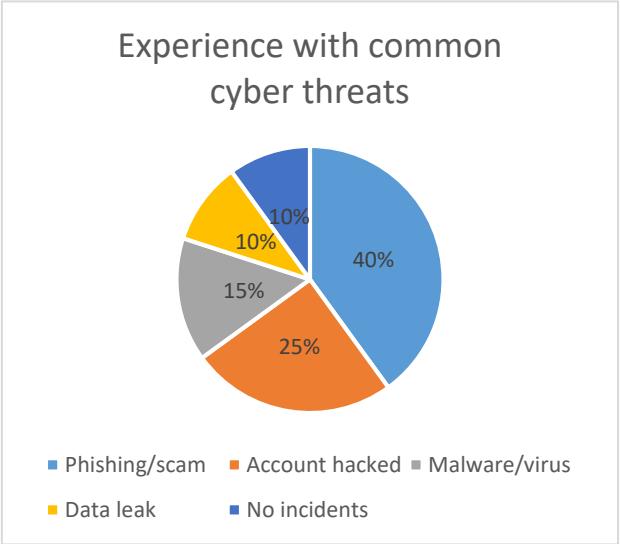

Figure 2

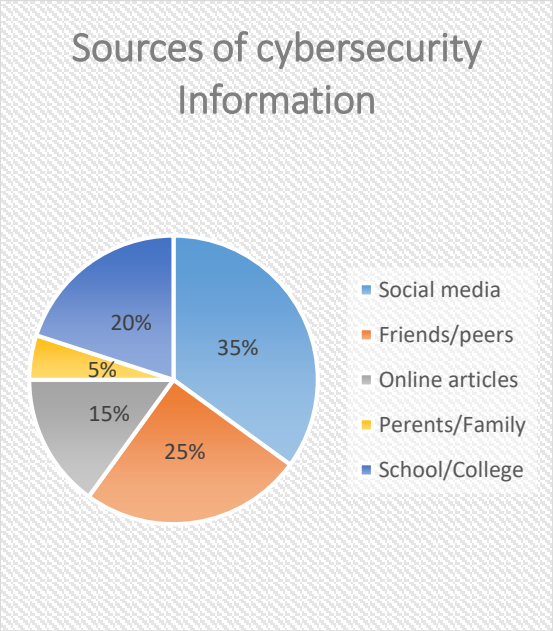

Figure 3

The data collected was analyzed statistically using both descriptive and inferential methods. Frequencies and percentages were calculated for the levels of awareness, prior experiences with threats, and levels of safe practice online. Composite indices were developed to measure overall cyber security awareness. The analyses showed that 30% of respondents had high levels of awareness; 45% had moderate levels, and 25% had low levels of awareness. This is illustrated in Figure 1, which indicates that many Gen Z individuals fall within moderate levels of awareness, indicating structured awareness programs are required in educational institutions.

RESULTS:

Figure 1: Overall Cyber security Awareness Levels of Gen Z

Additionally, when participants were asked about which types of cyber threats they had experienced personally, phishing messages and social media account hacking were reported most often. In Figure 2, approximately 40% of respondents reported receiving phishing or scam messages; 25% reported account hacking; 15% reported malware or virus attacks; while 10% reported being a victim of data leaks or identity theft; another 10% reported not having any cyber incidents. This shows that phishing and hacking continues to be issues with young digital users.

Figure 2: Encountering Common Cyber Threats by Gen Z

The survey also analyzed how Gen Z gets their cyber security education and awareness. The results, which can be found in Figure 3, indicated that 35% of respondents base their current knowledge of cyber awareness from social media awareness posts, 25% learn from their peers or friends, 20% learn through school/college workshops, some through online articles and videos (15%), and only 5% from family. Social media appears to have the biggest influence in building cyber awareness education among this generation.

Figure 3: Cyber security Learning Sources

Analysis of Online Behavioral Data. Observation of Gen Z user's online behavior was also conducted in addition to the survey to consider how users approach privacy and security practices on social media platforms. Publicly available social media posts and metadata were collected (consistent with the terms of consent) through platforms Instagram, X (Twitter), and YouTube. The analysis was to assess the frequency of posts related to privacy, the public evident sharing of personal data, and the existence of account privacy settings. Although many respondents claimed to practice good habits, there were

contradictions of the behavior observed online. An example would be some of the users who claimed, they always use strong passwords were frequent offenders of frequently reusing their passwords across multiple platforms or sharing too much personal details publicly. An online survey has been carried out among members of Gen Z between the ages of 18-26 to evaluate their comprehension of cyber security topics as well as their password behaviors, knowledge of multi-factor authentication (MFA), and experience with online scams. The survey results were then compared to findings from published reports from Yubico (2024) and EY Consulting (2022). It is documented that through the research, 62% of Gen Z population have either been taken in or interacted with a phishing scam and only 30% update their passwords or software regularly (Data economy, 2025). Around 40% indicated that they have never participated in any cyber security training and less than true half of the respondents participate in using MFA (MULTI FACTOR AUTHENTICATION) across all their accounts (Yubico, 2024). This data serves as a basis for understanding awareness gaps and behavioral risks. Education-based interventions are then developed based on the data; which included gamed simulations, interactive training modules, and micro-learnings on threat information as it relates to the real world. The program is then evaluated for effectiveness through pre and post training surveys for changes in awareness as well as behavioral shifts. The integration of both research reports and survey data indicates that Gen Z is proficient with technology, but their awareness of cyber security threats is uneven. Additionally, their overconfidence with digital skills are rationalized to minimize the importance of maintaining simple security practices like password management and phishing awareness. Thus, a data driven as well engaging awareness strategy that engages with real-life scenarios and short training modules with some form of continuous purchase is needed.

DISCUSSIONS:

Generation Z (born approximately between 1997 and 2012), the first generation to be raised entirely in a digital world, is constantly interacting with smartphones, social media sites, online gaming, and cloud computing applications, enabling unparalleled technology proficiency. Despite this, their knowledge and behavior surrounding cyber security awareness exhibit wide variations.

1. Factors Leading to Low Cyber security Awareness

- **Overconfidence in Digital Skills**

Many Gen Z think they are technology proficient, leading to a relaxed attitude towards basic security measures. For example, only 30% of respondents regularly update passwords or software while still displaying high proficiency using an app or device, with less than 50% using multi-factor authentication for every account.

- **Less Formal Education on Cyber security**.

Approximately 40% of Gen Z respondents have never participated in any form of cyber security education. Educational institute have computer literacy components in education. Competency in using an online service is not the same as practicing cyber security both at work and personally; Phishing, malware, and safe password practices tend to be omitted from curricula or overlooked entirely.

- **Exposure to Risky Online Environments**

Social media applications, online games, and free-content sites expose Gen Z to scams and phishing attempts. Online transactions and peer-to-peer environments heighten exposure to risks, where 62% of respondents claim to have interacted (even unknowingly) with a phishing scam.

- **Behavioral & Psychological Factors**

A culture of instant gratification can lead to rapid clicks and willingness to share personal information without much consideration. Gen Z has a tendency to underestimate potential risk. This attitude often contributes to neglecting baseline education, such as noticing software updates, using strong passwords, or enabling multi-factor authentication (MFA).

2. Contributing Factors to High Cyber security Awareness

- **Access to Information & Digital Literacy**

Gen Z has been exposed to lots of information online, including tutorial videos, online articles, and news pertaining to cyber security. Occasionally awareness of large breaches, hacks, or compromised emails and viral phishing campaigns influence them to behave more securely, such as by using MFA or a password manager.

- **Familiarity with Security Products**

Many people are willing to use familiar built-in security features of their devices (such as app permissions and two-step verification), even if these options are not always applied for the sake of security. Prior exposure to tech and having technical literacy results in quicker adaptation to new cyber security products if properly educated.

- **Peer Effect & Social Learning**

Talking with peers about online safety, scam experiences, or compromised accounts can raise awareness about cyber security risk. Gamed training, online videos, and interactive online information products are likely to be the most beneficial for this generation, as they tend to represent learning style preferences.

3. Implications

The mixed picture of awareness reveals that being tech-savvy does not convert into safe behavior. While Gen Z might easily traverse theoretically complex digital spaces, their understanding of risk and ability to implement harm full behaviors were found to be mixed. High awareness tends to exist when people have experienced actual threats or formal training. Low awareness occurs where overconfidence, lack of education, and/or behavior biases suppress attention to the basic cyber security protocols.

4. Recommendations

Data driven and engaging training is critical: gamed modules, micro-learning, and simulated experience of threat scenarios increase knowledge retention and understanding.

Behavior change over knowledge change: Understand that students need to be taught about change every day: MFA - you cannot use old shoes: how often we update and vigilant behaviors.

Continued reinforcement: short, repeated training, notifications, or campaigns are great reinforcement of safe habits online.

In short, Gen Z's cyber security awareness is uneven at best. In particular, their strengths in technology use are overconfident and influenced by limited formal education, resulting in risk-taking behavior. The good news is awareness can improve when we closely modify delivery, focus learning on knowledge AND behavior and work with audience members at a consistent frequency and duration.

4.1 Recommendations for Cyber security Awareness Programs:

To bridge these gaps, awareness programs should be informed by data, provide engaging experiences, and be tailored to Gen Z's digital habits and learning style.

- **Gamed Cyber security Simulations**

Interactive, scenario-based games where participants are given the task of identifying phishing attempts, malware, or insecure practices. Aids in developing skills in a real-life situation, but low-risk, engaging setting.

- **Micro learning Modules**

Short, more focused lessons (1-5 minutes long) about the content such as:

How to create solid passwords
How MFA works
Tactics used in social engineering
Fits to Gen Z's mobile-first, fast-paced life.

- **Real Life Scenario Training**

Employing real-life case studies of current hacks, influencers being taken advantage of, or scams using popular platforms and showing the direct relevance induces a sense of urgency to attend to cyber security.

- **Tweaks & Reminders with Behavioral Nudges**

Automated push notifications on mobile devices and reminders using email or social channels where Gen Z spends their time encouraging them to change passwords, enable MFA, or do not click links they deem suspicious.

- **Peer-influenced Learning**

Serve as user advocates where influencers/ reminders/ other community leaders rally for their community and ultimately potentially drive behavior changes towards more secure practices. Ultimately, it becomes a cultural norm for individuals to heed messages from trusted individuals.

- **Tracking Progress & Rewarding/Recognition**

Making tracking progress part of the learning with badges, leaderboards, or completing a module providing a certificate. Created to maintain/make it worth human traveler's while to confront behavior protocols for motivation and retention.

CONCLUSION:

Despite Gen Z's high levels of connection and digitally fluent, their cyber security practices do not match the dangers of online exposure. Without tailored education, their trust in technology may continue to obscure dangerous gaps in understanding. The answer is not more granular or longer training instead, they need engaging, practical and behaviorally informing awareness programs that meet Gen Z where they are, and evolve as new threats arise.

REFERENCE

1. Data Economy (2025), "Cybercrime trends and phishing exposure among young internet users", Data Economy Research Reports, Annual Report
2. Yubico (2024), "Global State of Authentication Security Report", "Cyber security and Generation Z: Awareness and behavioral risks", Ernst & Young Global Limited, Industry Report.
3. Pew Research Center (2023), "Teens, social media, and digital privacy", Pew Internet & Technology Reports, Survey Report.
4. ENISA (2022), "Cyber security awareness and behavior of young internet users", European Union Agency for Cybersecurity, Annual Report.
5. OECD (2021), "Educating youth for digital security and resilience", Organisation for Economic Co-operation and Development, Policy Report.
6. Alotaibi, F. (2021), "Cyber security awareness among university students", International Journal of Advanced Computer Science and Applications, Volume 12, Issue 4.
7. Ng, B. Y., McCoomb, S. A. & Wong, C. Y. (2020), "Cyber security awareness and behaviour of young adults", Information & Computer Security, Volume 28, Issue 3.
8. Kaur, K. & Singh, J. (2020), "Impact of cyber security awareness programs on user behaviour", Journal of Cyber Security Technology, Volume 4, Issue 2.
9. Tandon, A., Dhir, A. & Mäntymäki, M. (2020), "Why do people share fake news? Associations between social media use and misinformation", Journal of Retailing and Consumer Services, Volume 63.
10. Pattinson, M. et al. (2019), "Cyber security behavior: A review of protective and risky online actions", Computers & Security, Volume 87.
11. Bada, M., Sasse, A. & Nurse, J. (2019), "Cyber security awareness campaigns: Why do they fail to change behaviour?", Information & Computer Security, Volume 27, Issue 2.
12. Hadlington, L. et al. (2017), "Cybercognition: Cyber security awareness and risky online behaviour", Computers in Human Behavior, Volume 66, pp. 327–335.
13. Baruh, L., Secinti, E. & Cemalcilar, Z. (2017), "Online privacy concerns and privacy management: A meta-analytical review", Journal of Communication, Volume 67, Issue 1.
14. Parsons, K. et al. (2017), "The human aspects of information security questionnaire (HAIS-Q)", Computers & Security, Volume 42.
15. Vishwanath, A. (2016), "Habitual Facebook use and its impact on getting deceived by phishing attacks", Journal of Computer-Mediated Communication, Volume 21, Issue 1.
16. Shillair, R. et al. (2015), "Online safety begins with you: Age differences in cyber security behaviors", Computers in Human Behavior, Volume 50.
17. Livingstone, S. & Smith, P. (2014), "Annual research review: Harms experienced by child

users of online technologies", Journal of Child Psychology and Psychiatry, Volume 55, Issue 6.
18. Crossler, R. E. et al. (2013), "Future directions for behavioral information security research", Computers & Security, Volume 32.
19. Furnell, S. & Clarke, N. (2012), "Power to the people? The evolving recognition of human aspects of security", Computers & Security, Volume 31, Issue 8.
20. Dinev, T. & Hart, P. (2006), "An extended privacy calculus model for e-commerce transactions", Information Systems Research, Volume 17, Issue 1.

HOW TO CITE: J. Anurushmitha*, D. Nikhitha, J. P. Pramod, Cyber Security Awareness Among Genz, Int. J. Sci. R. Tech., 2026, 3 (3), 159-167. https://doi.org/10.5281/zenodo.18928049