INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

A Review on Disparity of Cyber Security between Different Age Brackets in India; with Imminent Cyberthreat Challenges each Bracket Suffers

[1]Nobex Wahengbam, [2]Dr. Murugan R, [3]Tannaz Mahreen

MCA Student, School of Computer Science and IT., Jain (Deemed-to-be University), Bangalore, India[1]

Programme Head-MCA, School of Computer Science and IT., Jain (Deemed-to-be University), Bangalore, India[2]

BA(H) Philosophy Student, Department of Philosophy., Indraprastha College for Women, University of Delhi, Delhi, India[3]

ABSTRACT: With the exponential growth of digital technologies, understanding the nuanced differences in cybersecurity awareness, practices, and vulnerabilities among different age groups becomes imperative. This study illuminates the elements that contribute to the cybersecurity gap by doing a thorough examination of current literature, papers, and empirical research. It explores the role of technological literacy, access to resources, socio-economic status, and cultural attitudes in shaping cybersecurity and cyber awareness and the preparedness among different generations. Furthermore, the review identifies key challenges hindering effective cybersecurity measures and underscores the implications of these disparities on national security and individual privacy. By illuminating the disparities and challenges, this paper calls for tailored cybersecurity strategies to bridge the gap across the awareness and importance of security in the cyber security for self in all age brackets, ensuring a safer digital environment for all citizens in India.

KEYWORDS: age group, technological literacy, cyber awareness, preparedness, disparites

I. INTRODUCTION

In the rapidly evolving realm of cybersecurity, comprehending the differences among age groups is essential for devising effective strategies to protect digital environments. India has experienced a significant increase in internet usage and digital integration across all age groups, underscoring the importance of examining varying levels of cybersecurity readiness and vulnerabilities. This review aims to explore the complex dynamics of cybersecurity across different age groups in India, shedding light on existing disparities and challenges within this context.

The widespread adoption of digital technologies has transformed the way people communicate, work, and transact. However, this digital revolution has also brought about a multitude of cybersecurity risks, including malware, phishing attempts, data breaches, and identity theft. While efforts have been made to enhance cybersecurity awareness and infrastructure, their impact can vary greatly across different age demographics.

Understanding the factors influencing the cybersecurity gap among age groups is crucial. Variables such as familiarity with technology, access to resources, socioeconomic status, and cultural attitudes significantly influence individuals' cybersecurity behaviours and resilience. Additionally, differences in digital proficiency and risk perception between generations exacerbate the difficulty of effectively addressing cyber threats.

This review aims to consolidate existing literature, reports, and empirical studies to offer a comprehensive analysis of the cybersecurity landscape across age groups in India. By identifying prominent challenges and disparities, this paper seeks to inform policymakers, industry stakeholders, and educators about the pressing need for tailored cybersecurity measures that cater to the distinct requirements and vulnerabilities of various age cohorts. Ultimately, by bridging the cybersecurity divide across generations, India can strengthen its cyber defences and ensure a more secure digital environment for all its inhabitants.

II. HYPOTHES

The hypothesis proposes that the diverse range of cybersecurity vulnerabilities and readiness among India's age groups can be attributed to a complex interaction between a number of factors, including cultural attitudes, socioeconomic status, technological familiarity, risk perception, and resource accessibility. With the ever-changing digital environment and rising internet usage, this study attempts to examine these complex dynamics. The hypothesis posits that generational inequalities in these critical characteristics account for persistent discrepancies in cybersecurity

knowledge and resilience, based on a synthesis of existing research, reports, and empirical studies. The goal of the analysis is to find trends that illustrate the unique difficulties that different age groups encounter when dealing with cybersecurity risks. Moreover, the study suggests that a thorough comprehension of these variables will guide the creation of customized cybersecurity defenses. The ultimate objective is to close the cybersecurity gap that exists in India between different age groups by giving educators, industry stakeholders, and policymakers the knowledge they need to put effective initiatives into practice. As a result, it is anticipated that the country's cyber defenses will be strengthened and that everyone will live in a more secure digital environment, meeting the needs of the rapidly changing technological world.

III. PROPOSED METHODOLOGY

This paper uses an amalgamation of both primary and secondary sources to provide a comprehensive overview

A. *Primary Sources:*

- Semi-structured interviews with people of various age brackets serve as the primary data collection method. The researchers conducted the interviews both in person and over the phone. The questions were designed to garner detailed and comprehensive responses, and the interviews were recorded and transcribed for future analysis.

Primary Sources

- Qualitative research techniques will be employed to analyze the information gathered from the literature review and interview data. To find patterns and themes connected to the study hypothesis, it will be arranged, coded, and analyzed.
- The approach described above will give readers a thorough grasp of the problem, and the combination of primary and secondary sources will guarantee a thorough and impartial analysis of the topic, giving the research paper a strong foundation

Subject 1
Name: Anonymous
Sex: Female
Date and Time of Interview: 1st of February, 2024; 9:25 am (IST)
Medium: In-person
Interviewer: Tannaz Mahreen
I: Please state your name, age and occupation.
S: Redacted to uphold anonymity, (age 33).
I: Sounds great, what are your means of income?
S: I work as household help in people's homes.
I: Very well, now, what phone do you use, Ma'am?
S: I use a Spice phone, the one with buttons?
I: Yes, yes, I understand. How would you describe your financial situation?
S: (stays silent)
I: Please be comfortable, you do not have to answer anything that makes you uneasy.
S: Let's just say that I am barely managing.
I: I see, very understandable. Now, may I know if you use any locks on your phone? Like a password or something?
S: No, no, nothing like that.
I: How do you keep your phone safe, then?
S: I just keep it close to me when I walk around.
I: So that it doesn't get stolen?
S: Yes, yes
I: Okay, now, what are the minorities you belong to?
S: Well, I am a woman,
I: Yes?

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203015 |

S: I am also a Muslim from the Dalgaon Village in Mangaldoi (a district in Assam),

I: Yes, yes and is Assamese your first language?

S: No, no, it is Bengali.

I: Because of belonging to these communities would you say that you face any difficulties?

S: In my daily life? Yes, yes.

I: Got it, now, Miss, do you know what a virus is?

S: No, no, I don't.

I: Have you heard of computers getting attacked by viruses?

S: I have heard of people talking about it, but I haven't seen it myself.

I: But, you have heard people talk about it?

S: Yes, that I have.

I: I see, and do these discussions happen very often in your social circles? Regarding computer security?

S: I mean, I have heard people talk about it but I haven't had any personal experience with it.

I: Got it. Miss, have you shared your card details with anyone? Provided you have an ATM card?

S: Yes yes, I have an ATM card and Passbook and all. I haven't shared the details with anyone, I mean my husband knows, but no one else.

I: But, your husband knows?

S: Yes, he does.

I: Okay, I see, do you frequently receive calls or texts from random numbers asking if you need friends or that you have won great amounts of money?

Paper id Journal of Emerging Technologies and Innovative Research (JETIR) www.jetir.org 28

S: Not calls, but I do get texts sometimes. But, my phone is small so I haven't been able to do anything about them.

I: Yes, yes, do you use the internet? For Facebook or anything?

S: No, no, my phone doesn't have all that.

I: Got it. Now, these questions that I asked you; do you think you would have answered them differently if you were in a different social and economic position?

S: If I were rich?

I: Yes, if you were a very rich man living in America, would you have answered these differently?

S: Yes, that would be a very big person and I don't know how to read and write so of course I would have answered all of these questions much better.

I: You have already done a great job, thank you very much for your cooperation. Is it alright with you if we use this recorded interview for our research?

S: Yes, please, go ahead. I hope it is useful.

Subject 2

Name: Tasaduk Ariful Hussain

Sex: Male

Date and Time of Interview: 10th of February, 2024; 10:40 am (IST)

Medium: Telephonic

Interviewer 1: Tannaz Mahreen

Interviewer 2: Nobex Wahengbam

I1: Please state your name, age, and occupation.

S: My name is Tasaduk Ariful Hussain. My age is fifty six and my occupation is that I am a consultant in the development sector.

I2: Okay, okay, how are you today, Mr. Hussain?

S: I'm good, I'm good, feeling good about the interview.

I2: Okay so the next question we'd like to ask is; which mobile phone do you own, sir?

S: I use a Samsung Galaxy M20.

I2: Okay, sir, are you aware of which operating system it has?

S: Uh, I think it is android?

I2: Okay, are you aware of screen locks, sir?

S: Sorry?

I2: The locks we use on our phones before we use them. Like a fingerprint lock or a pin, do you use any of these?

S: Oh yes, yes, I use a pattern form of lock.

I1: Very well, Mr. Hussain, how would you describe your financial status?

S: Hmm…do you have any options?

I1: Let's go on a scale of 1 to 10, 5 being the poverty line.

S: I would say an 8.

I2: Got it. Sir, are you aware of what viruses are?

S: Yes, yes, I'm aware of them.

I2: Great, could you perhaps tell me the types of viruses?

S: No, I'm afraid not, I don't know the types.

I2: Okay sir, no problem. If you're aware of viruses have you also heard of antiviruses?

S: Yes, I have.

I2: Do you know what antivirus does?

S: I think it protects something called a firewall if there is any virus trying to enter my phone or my laptop. It blocks viruses, I believe. Occasionally I run my entire hard disk and memory system through the antivirus so that if there is any virus it can remove or quarantine it.

I2: Yes, sir. Is there any specific antivirus you use?

S: Yes, Malwarebytes.

I1: Very well, sir. Are you a part of any minorities?

S: Yes, I am from a religious minority. Secondly, I am from the North-Eastern states of India which are often privy to discrimination because of their largely Mongoloid population.

I2: Okay, okay. Sir, are you aware of what 2FA means in security?

S: No, no. I don't.

I1: No problem, sir. Have you ever been contacted by a suspicious scammer, Mr. Hussain? And could you please describe your experience if you have?

S: A scammer? Yes, yes. Once I was messaged and immediately video called by a girl and when I picked up the call she started stripping off her clothes. I cut the call but she then sent me screenshots with my face on the call and blackmailed me to post it onto my social media if I didn't send some lakhs of money. I immediately went to the police station to file an FIR. There was another guy who called under the pretext of being the DGP of the Cyber-Crime division of Delhi Police and he threatened me saying that I was doing something illegal. So, I decided to take even more prompter action.

I1: Okay, and what was the response like from the police?

S: I haven't been informed of the actions they have taken after the FIR but, they were receptive and explained the situation saying that it was very common and I was not to panic.

I2: Okay, okay, sir. Sir, have you ever shared your card details with anyone for any purchase or any other reason?

S: Yes, with family members for purchases and stuff. Once with my daughter, a couple of times with my wife, and once with my son, as well.

I1:Okay, very well. Sir, are there any conversations about IT Security in your social circles?

S: Um, not much. Once in a while, I bring up this issue but, there isn't much awareness in my circles. I sometimes get emails and Whatsapp forwards about IT security, and that's about it.

I2: Speaking of security, have you ever been the subject of any form of hacking or data breach?

S: Um… not that I'm aware of, no.

I2: Got it. So have you ever connected to any open Wi-Fi in public? The Wi-Fis without any password?

S: Yes, yes, on some occasions. Like, at the airport or metro stations in Delhi.

I1: Okay, so for the last question of the day, sir; do you think, Mr. Hussain, that your social privilege has an impact on your IT security?

S: I think yes, it does. For two reasons; first, I have a decent mobile phone which supports VPN and the economic means to afford security. Secondly, I'm an educated person and bother to go through measures to secure myself when it comes to IT.

I1: Very well, I'd like to run a few clarifications by you, if that's okay with you, Mr Hussain?

S: Yes, yes, please go ahead.

I1: Are you aware that this call is being recorded, sir?

S: Yes, I am aware.

I1: Do you consent to the use of the contents of your interview to be used in our research?

S: Yes, of course.

I1: Very well, you will be contacted shortly with the completed findings of the research and a transcript of your interview. Thank you very much for your time and contribution. We are greatly appreciative of it.

S: Thank you and best of luck with this very interesting research that I'm sure will help many people.

Subject 3

Name: Rohnak Kabrabam

Sex: Male

Date and Time of Interview: 13th of February, 2024; 10:40 pm (IST)

Medium: In-person

Interviewer: Nobex Wahengbam

I: Please state your name, age, and occupation.

S: My name is Rohnak Kabrabam. I am currently 23 running. Pursuing MCA in Jain University

I: Which mobile do you own? And does it have Android or iOS?

S: I own Samsung Galaxy S22 and Google Pixel 8. Both has Android.

I: Okay, sir. Do you use any form of screen locks?

S: Yeah, I'm using face ID in Pixel and fingerprint lock for Galaxy S22.

I: So it is a form of security. Okay.

I: So how would you describe your financial status?

S: My father has been in the industry. He's the head of the department. So he sends me around five thousand per month.

I: Alright, moving on. Have you ever downloaded and used third-party software on your device?

S: No, no.

I: Do you know what is 2FA?

S: You mean, authenticator?

I: Yes, the two FA authenticator. Do you know that, sir?

S: Yeah, I'm using that.

I: Do you use it for any email?

S: Yeah, in Gmail, I'm using.

I: Okay, sir. And do you regularly partake in conversations about IT security in your social circles?

S: No.

I: So do you know what are the types of viruses?

S: Yes, I know. Yeah. I know, of three types malware, trojan, and worm.

I: Okay, sir. And do you know what is antivirus?

S: Yes. It prevents that virus that I mentioned.

I: Could you be a bit more specific about what antivirus is?

S: Like, to protect your personnel things like files, and they also prevent the corrupting of your system, and it allows us to search the browser in a secure way.

I: Okay, so what kind of antivirus do you use?

S: I use Norton 360.

I: So, have you ever shared your card details? Anyone?

S: No.

I: Not even your family, sir?

S: I have shared the card with my father.

I: Are you a part of any minorities?

S: No, I'm Hindu.

I: Okay, so have you ever been contacted by any suspicious scammer?

S: Yeah, I got so many calls from the scammer.

I: So could you elaborate on one of the situations in a very brief manner?

S: It's like they're told me like, I got an offer for a job in foreign companies that actually paid around one lakh, something like that. But I didn't believe that. So I refused to call back.

I: Have you ever been hacked or had any data breaches?

S: Yeah. Last time, my game account has been hacked by some Russian hacker.

I: Okay, sir. So have you consulted any Cyber Security Analyst for the account that has been hacked?

S: Yes, I have contacted the company of that game. So they told me like to wait around one week some longer, but it didn't happen.

I: So there was no reciprocation from the company?

S: No

I: Okay, sir. So have you ever connected to any open Wi-Fi in the public?

S: Yes.

I: And do you think your social privilege has any impact on your security?

S: Yeah, I'm using this device, iPhone, but it's more secure to us than Android. Also, iOS has so many authenticator app like Apple authenticator is there. And they also have, the app also has email or trying to get something like that. And I also join so many IT seminars. They give me security tips like how to prevent a cyber-attack from a hacker.

I: Okay, sir. So do you want a recording of our interview, sir?

S: Yeah.

I: And so do your consent for our conversations to be used in our research paper?

S. Yes.

I: Okay, so thank you, sir.

Subject 4
Name: Tasaduk Trehan Hussain
Sex: Male
Date and Time of Interview: 18th of February, 2024; 05:40 pm (IST)
Medium: Telephonic
Interviewer: Nobex Wahengbam.

I: Please state your name, age, and occupation.

S: My name is Tasaduk Trehan Hussain, 16 years old as of this year and will be giving my 10th boards this year.

I: Which mobile do you own? Does it have Android or iOS.

S: I own a Samsung Galaxy A03 Core, it's is an Android.

I: Do you use any form of SCREENLOCKS?

S: Yes, I do

I: What is antivirus? And which do you use?

S: I use an anti-virus called "AVG anti-virus"

I: I see, and can you tell me what are the types of viruses if you have any knowledge about it?

S: I don't know of many; I've just read about Worms and Trojan horses in my IT book. Other than that idk any

I: Do you use 2FA for your important email id?

S: I don't know what that is

I: Have you ever shared your Card details to anyone?

S: I don't have my card, my parents do, so I think they know my card details.

I: Have you ever downloaded and used third party software in your handheld device or your laptop/desktop?

S: I'm not sure what a third-party software is, but if it is apps like Discord, Spotify, Krita etc, then I have.

I: Have you ever been contacted with suspicious scammer?

S: I lowkey got scammed into some free dairy milk ad. Lol I don't know if that counts.

I: Have you been hacked and had data breach in the past?

S: Nope, never been hacked before.

I: Have you ever connected to any open Wi-Fi in the public?

S: Yes

I: Okay, sir. So, do you want a recording of our interview, sir?

S: Yeah.

I: And so, do your consent for our conversations to be used in our research paper?

S. Yes.

I: Thank you for your time.

B. *Secondary Sources:*

To find pertinent literature on the topics of security in IT and Awareness, a thorough review of the literature was carried out. Academic publications such as journals, books, and reports are included in the literature review, along with online resources like forums and blogs. It focuses on how cyber security is currently doing, how the awareness and education on digital security precedes, what the people of the various demographics with concerns to age should atleast comprehend digital security, and how digital disparity has consequences.

IV. PRIMARY FINDINGS

Age brackets and the generations involving the brackets often exhibit significant disparities in cybersecurity awareness and practices due to varying levels of digital literacy and experience. The digital landscape presents a fascinating tapestry of challenges and opportunities, woven with threads of varying thickness and texture according to age. While the internet serves as a common ground, diverse generations traverse it with distinct levels of cybersecurity awareness and practices, highlighting a critical digital divide.

Younger generations, particularly digital natives who have grown up immersed in technology, may possess a greater familiarity with digital platforms and devices, yet they can also be more prone to engaging in risky online behaviours such as sharing personal information without considering the consequences or clicking on suspicious links.

This generation often dubbed "digital natives," wield technology with an almost innate familiarity. Growing up alongside the internet, they possess a fluency in navigating online platforms and possess a certain comfort with its intricacies. However, this comfort can sometimes translate to complacency, potentially leading to overlooking subtle security risks. Phishing scams, for instance, might appear less obvious to those accustomed to the fast-paced flow of online information, making them more susceptible. This overconfidence can make them vulnerable to cyber threats like phishing attacks and malware infections.

Conversely, older age groups may have less exposure to technology and therefore be less adept at recognizing cyber risks or implementing security measures. They may struggle with understanding complex privacy settings or recognizing the signs of a scam. Additionally, older individuals may face challenges in adapting to rapidly evolving technologies and may be more susceptible to falling for scams or phishing attempts due to a lack of experience or exposure to digital platforms. Older generations, often termed "digital immigrants," approach the digital world with a cautious curiosity. While their understanding of technology evolves, some might lack the technical proficiency or confidence to explore its full potential. This cautiousness, however, can translate into a heightened awareness of potential threats. They might be more likely to scrutinize emails, double-check website legitimacy, and hesitate before clicking on unknown links. However, this vigilance can sometimes morph into suspicion, hindering their ability to fully reap the benefits of online resources and services.

V. LITERATURE REVIEW; DISCUSSION AND ANALYSIS:

Above explains the context of the disparity in a fashion more stitched of generational. Next the dive onto the disparity with more focus on the age brackets between 0 to 18, 18 to 28, 28 to 48, 48 and above.

Between the age of zero to eighteen: 0-18: Digital Natives, Untamed and Untested

Children born after the year 2000, aptly named "Generation Alpha," have technology woven into the fabric of their lives. They're internet natives, effortlessly navigating digital platforms. However, this comfort can be a double-edged sword. Familiarity breeds complacency, potentially rendering them susceptible to threats like cyberbullying, online predators, and inappropriate content. Studies reveal that over 60% of children aged 8-12 have encountered cyberbullying, highlighting the need for early intervention. In 2022, the FBI's Internet Crime Complaint Center received over 8,000 reports of online victimization against minors, emphasizing the urgency of robust parental controls, age-appropriate education, and open communication within families.

Cyberbullying casts a long shadow, with studies by the Cyberbullying Research Center revealing that over 60% of 8–12-year-olds have experienced it. The scars can be severe, impacting mental health, academic performance, and even leading to self-harm. Parental controls and open communication are crucial first lines of defense, coupled with age-appropriate education programs that teach children how to identify, report, and cope with cyberbullying.

Online predators lurk in the shadows of seemingly innocent platforms, posing significant risks. The FBI's Internet Crime Complaint Center received over 8,000 reports of online victimization against minors in 2022 alone, highlighting the urgency of awareness campaigns and proactive steps. Equipping children with digital literacy skills, teaching them about safe online behavior, and encouraging open communication with trusted adults are vital to keeping them safe.

Inappropriate content permeates many corners of the online world, exposing young minds to potentially harmful or age-inappropriate material. Parental controls and filtering software offer a level of protection, but ultimately, open communication and critical thinking skills are crucial. Educating children to be discerning consumers of online content, encouraging them to question and discuss what they see, and fostering healthy skepticism are essential in navigating this complex landscape.

Between the age of eighteen to twenty-eight: 18-28: Digital Nomads, Risk-Takers and Trendsetters

Generation Z, born between 1997 and 2012, are the true digital nomads, constantly connected and plugged into the ever-evolving online world. Social media giants like TikTok and Instagram hold immense sway, making them highly responsive to online trends and challenges. However, this constant connectivity exposes them to unique cybersecurity risks.

Privacy Concerns: The Facebook-Cambridge Analytica data scandal in 2018 exposed the vast amount of personal data collected online. Gen Z is increasingly aware of privacy issues, with platforms like Signal and DuckDuckGo gaining popularity. Educating young adults about data privacy settings, encouraging the use of strong passwords and multi-factor authentication, and promoting awareness of data collection practices empower them to make informed choices about their online identities.

Pressure to Curate: The "Instagram vs. Reality" movement highlights the unrealistic portrayals on social media. Studies show a link between excessive social media use and increased anxiety and depression in Gen Z. Promoting body positivity, encouraging self-acceptance, and fostering critical thinking about online portrayals are key. Mental health resources like the Trevor Project and Crisis Text Line offer support and guidance.

Cybersecurity Threats: In 2023, phishing scams targeting online banking credentials saw a significant rise. Gen Z's trust in online information can make them susceptible. Gamified educational initiatives like "CyberStart" simulate real-world scenarios, teaching them to identify phishing attempts, verify online sources, and practice safe online behavior.

Between the age of twenty-eight to forty-eight: 28-48: Digital Immigrants, Cautious Learners and Multitaskers

Generation X, born between 1965 and 1980, remembers a world before the internet. Their digital journeys began later in life, fostering a cautious and measured approach. While not always tech-savvy, they often exhibit heightened awareness of potential threats, stemming from their initial distance from technology. However, this very distance can create challenges in the ever-evolving digital landscape.

Outdated Security Practices: A 2022 Google report revealed that 59% of adults reuse passwords across multiple accounts, a practice increasingly exploited by hackers. Upskilling programs like "Get Cybersecurity Savvy" offer practical workshops on password management, multi-factor authentication, and secure online practices, specifically designed for Gen X learners.

Difficulty Adapting to Platforms: The emergence of platforms like Metaverse and NFTs can leave Gen X feeling overwhelmed. Intergenerational learning initiatives like "Tech Grandparents" pair younger mentors with older learners to bridge the technology gap and foster digital inclusion. Libraries and community centers can also offer technology training workshops tailored to Gen X needs.

Fear of Missing Out: The rapid adoption of digital tools like online banking and e-commerce can create pressure to adapt. Promoting digital literacy and fostering open communication are key. Programs like "Senior Planet" offer workshops on online banking, smartphone basics, and navigating popular websites, empowering Gen X to confidently participate in the digital economy.

Age of forty-eight and above: 48+: Digital Skeptics, Navigating with Prudence

Baby Boomers, born between 1946 and 1964, and after often approach the internet with a healthy dose of skepticism. Their limited exposure to technology during their formative years translates into varying levels of comfort and confidence in the digital world. While this caution offers some protection from online threats, it can also hinder their ability to access essential online services and resources.

Limited Access to Technology: The AARP's Digital Equity Survey 2023 found that cost is a major barrier to internet access for older adults. Initiatives like Lifeline provide subsidized internet plans for low-income individuals, while community technology centers offer free Wi-Fi and digital literacy training. Affordable tablets and smartphones designed for seniors can further bridge the access gap.

Digital Literacy Challenges: Many older adults lack basic knowledge of online security concepts like malware and phishing. Age-appropriate programs like "AARP Fraud Watch" offer interactive workshops and resources specifically tailored to seniors' learning styles, teaching them to identify online scams, protect their personal information, and navigate the online world safely.

Fear of Fraud and Scams: The "grandparent scam" preys on seniors' trust and sense of urgency. Public awareness campaigns like "Stop Senior Scams" educate older adults about common scams, promote safe online behavior, and encourage them to report suspicious activity to trusted individuals or authorities.

VI. CONCLUSION

While the internet serves as a shared canvas, our experiences on it differ vastly based on age. From the untamed enthusiasm of young natives to the measured skepticism of digital immigrants, each generation navigates the online world with distinct strengths and vulnerabilities. Bridging the cybersecurity divide isn't a one-size-fits-all solution; it requires acknowledging these disparities and weaving a tapestry of collaborative efforts. Tailored education programs, intergenerational knowledge sharing, and equitable access to technology and resources are the threads that bind us. Ultimately, our goal is to empower individuals of all ages to become responsible citizens of the digital world, creating a vibrant and secure tapestry where every thread represents a voice empowered to navigate the online space with confidence and safety. This journey requires continuous learning and adaptation, but by working together, we can ensure that the digital future is inclusive and secure for all.

REFERENCES

1. Nicholson, J., Coventry, L., & Briggs, P. (2019, May). " If It's Important It Will Be A Headline" Cybersecurity Information Seeking in Older Adults. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-11).
2. Khan, N. F., Ikram, N., & Saleem, S. (2023). Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. Security Journal, 1-31.
3. Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019, December). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities. In Journal of Physics: Conference Series (Vol. 1339, No. 1, p. 012098). IOP Publishing.
4. Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring age and gender differences in ICT cybersecurity behaviour. Human Behavior and Emerging Technologies, 2022.
5. Herdiyanti, A., Adityaputri, A. N., & Astuti, H. M. (2017). Understanding the quality gap of information technology services from the perspective of service provider and consumer. Procedia Computer Science, 124, 601-607.
6. Jones, S. L., Collins, E. I., Levordashka, A., Muir, K., & Joinson, A. (2019, May). What is' Cyber Security'? Differential Language of Cyber Security Across the Lifespan. In Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-6).

7. Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. Information, Communication & Society, 21(5), 712-728.
8. Robinson, L., & Cotten, S. R. (2013). Digital inequality: A divide in need of bridging. New Media & Society, 15(5), 724-742.
9. Heeks, R. (2022). Digital inequality beyond the digital divide: Conceptualizing adverse digital incorporation in the Global South. Information Technology for Development, 28(4), 688-704
10. Molala, T. S., & Makhubele, J. C. (2021). The connection between digital divide and social exclusion: Implications for social work. Humanities & Social Sciences Reviews, 9(4), 194-201.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 **9940 572 462** 💬 **6381 907 438** ✉ **ijircce@gmail.com**

Scan to save the contact details