International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Recent Advances in Computer Applications and Information Technology
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Digital Literacy & Cybersecurity Awareness among Senior Citizens

Kashish Mendhe, Suhani Kumeriya

G H Raisoni University, Amravati, Maharashtra, India

Abstract

The way people get information talk to each other. Do financial things has changed a lot because of digital technologies. Governments, businesses and people who provide services are using platforms more and more to give people important services like banking, healthcare and social welfare programs. These new technologies have a lot of things about them but they also make things hard for some groups of people especially older people. So it is very important that older people know how to use technologies safely and understand how to protect themselves from cyber threats. Older people often have trouble understanding and using technologies, which makes them more likely to be victims of cyber threats like online fraud, identity theft and phishing scams.

Digital literacy is the ability to use technologies like computers, smartphones and the internet. It includes skills like navigating platforms talking to people through digital tools managing online information and understanding how to stay safe online. For people digital literacy is not just about technology it is also about being part of society and being independent. Many services like banking paying bills and getting care are moving online so digital literacy helps older people take care of themselves and be part of society. However many older people struggle with technologies because they do not have much experience with them they do not get enough training they have cognitive challenges or they are afraid of making mistakes. These things contribute to a difference between younger and older people when it comes to digital technologies.

One of the concerns about older people using digital technologies is cybersecurity. Cybersecurity is the protection of devices, networks and personal information from cyber threats like hacking, phishing and financial fraud. Older people are often seen as one of the vulnerable groups in cyberspace because they may not know much about online risks and safe digital practices. Cybercriminals often target people through fake emails, fake investment schemes and fraudulent phone calls. These scams often take advantage of peoples trusting nature or their limited knowledge of digital communication. In some cases cybercriminals create a sense of urgency or fear which convinces victims to give out information or send money. These attacks can result in financial losses and emotional distress for older victims.

Another challenge that affects cybersecurity awareness among people is the lack of knowledge about protective measures like creating strong passwords using two-factor authentication, safe browsing practices and recognizing phishing attempts. Many older people use devices mainly to talk to family members or do basic tasks like messaging and browsing. As a result they may not fully understand the risks that come with online activities. A study done in India found that peoples limited knowledge of cybersecurity practices makes them more vulnerable to financial scams and identity theft. The study also showed that experiences of cyber fraud can lead to stress and reduced confidence in using technologies, among older people. Digital literacy and cybersecurity awareness are very important for older people to safely use technologies and protect themselves from cyber threats. Older people need to know how to use technologies and how to stay safe online to maintain their autonomy and participate actively in society.

KEYWORDS*: Cybersecurity Awareness, Senior Citizens, Older Adults, Digital Inclusion, Online Safety, Cybercrime Prevention, Internet Usage Among Elderly, Digital Divide, Information Technology Adoption, Phishing and Online Fraud, Cybersecurity Education, Digital Skills Training, Data Privacy Protection, Technology Accessibility.*

1. Introduction

The way people talk to each other and do things has changed a lot because of technology. Senior citizens are using platforms like Facebook and WhatsApp to stay in touch with friends and family get medical help and do their banking. These online tools make life easier. Give them more freedom. They also make senior citizens targets for cyber threats that they do not fully understand. Because they do not know much about technology and have not had any formal training, they are more likely to fall for things like fake emails, online scams and identity theft. Sometimes cybercriminals pretend to be companies like Amazon to trick them. So it is really important that senior citizens know how to use technology safely. This means they need to be able to look at information and decide if it is true or not keep their personal information private and be careful when they are online.

If we want senior citizens to feel safe and confident when they are online we need to teach them about cybersecurity. It is also important for them to be able to use technology so they are not left out of things. When senior citizens do not know how to use technology they can feel lonely they might not be able to get the help they need and they might not be able to take part in their community.

Nowadays governments and other organizations are putting more and more of their services online. So senior citizens need to know how to use technology to get these services. If they do not get the help they need they might feel overwhelmed. Not want to use digital technology at all. This would make it even harder for them to get the things they need. At the time cybersecurity threats are getting more and more complicated. Scammers are using things like fear and trust to trick citizens into giving away personal information. They send emails and make fake phone calls that look like

they are from real organizations. So senior citizens need to know how to spot these scams and keep themselves safe.

They need to know things like how to make passwords, how to use two-factor authentication and how to keep their devices up to date. To deal with these problems we need to have a plan that includes teaching citizens about digital technology getting their family and community involved and making sure digital technology is easy for them to use. Community centers and family members can play a role in helping senior citizens feel confident when they are online. If we teach citizens about digital technology in a way that is easy for them to understand and give them plenty of time to practice they will be better at using digital technology and they will feel more confident.

If we encourage citizens to help each other learn about digital technology they will be more likely to keep using digital technology safely. We also need to make sure that digital technology is easy for senior citizens to use. This means making sure that the instructions are clear the security features are easy to use and the text is large enough to read. Technology companies should make their platforms more inclusive by adding things like voice assistance and simple privacy settings. Finally it is really important that senior citizens keep learning about technology throughout their lives. Cyber threats are always changing,. Senior citizens need to stay up, to date with the latest information to stay safe. If we give citizens the knowledge they need they will be able to protect themselves from online threats. They will also feel independent their self-esteem will improve and their overall quality of life will be better. By teaching citizens about digital technology getting their community involved and making sure digital technology is easy to use we can help them feel safe and confident when they are online.

Fig.1 Building Digital Resilience Among Older Adults"

2. Literature Review

The existing literature shows that literacy and cybersecurity awareness among senior citizens are serious problems in modern society which relies on digital technology. Digital literacy enables individuals to operate systems and cybersecurity awareness enables users to understand internet threats and implement protective measures.

Research shows that older adults have digital skills like messaging and browsing but they find it hard to assess online content and control their credential storage privacy settings and detect cyber threats. Their digital competence develops through their background and past experiences and self-belief and social network assistance. Seniors face risks of cybercrimes like phishing attacks and scams and identity theft because they lack security knowledge and display excessive trust and lack understanding of technical security methods. People with digital literacy skills will practice safer online behavior because they know how to use technology.

Customized training programs that combine exercises and user-friendly technology design lead to better digital abilities and improved security practices. Older adults need education programs and learning spaces that help them learn safe digital practices. Digital literacy and cybersecurity awareness among citizens remain serious problems in modern society which relies on digital technology. Digital literacy enables individuals to operate systems and cybersecurity awareness enables users to understand internet threats and implement protective measures.

Older adults have digital skills like messaging and browsing but they struggle with more advanced skills like evaluating online content and managing credential storage privacy settings and detecting cyber threats. Their digital competence is shaped by their background and past experiences and self-belief and social network assistance.

Seniors face risks of cybercrimes like phishing attacks and online scams and identity theft because they lack security knowledge and display excessive trust and lack understanding of technical safeguards. People with digital literacy skills practice safer online behavior because they know how to use technology.

Customized training programs that combine exercises and user-friendly technology design lead to better digital abilities and improved security practices among older adults. Older adults need education programs and dedicated learning spaces like community centers and libraries and senior clubs that provide safe environments where they can practice digital skills and ask questions and receive peer or mentor support. These spaces also foster inclusion and reduce isolation and reinforce safe digital habits.

Older adults need education programs rather, than one-time interventions to adapt to evolving technologies and increasingly sophisticated cyber threats. Dedicated learning spaces provide environments where older adults can practice digital skills at their own pace and ask questions without embarrassment and receive peer or mentor support.The Pew Research Center did a study on how older adults use technology. They found out that even though more seniors are using the internet now than they were ten years ago a lot of them still have trouble understanding how to use tools and online services. Older adults usually use devices to talk to their family members and friends. They like to send messages and make video calls.. They do not know how to use the advanced features on their devices.

This means that older adults are more likely to get hurt by cyber threats and online fraud. They do not know how to stay online.

Some other researchers, Choi and DiNitto did a study in 2013 on adults who are low-income and homebound. They found out that these older adults have limited skills and they do not have access to technology. This makes it hard for them to connect with people and it also makes it hard for them to get the things they need. The researchers said that digital literacy is important because it helps older adults navigate the internet safely. Older adults who are good at using devices can use online health resources and government services. They can also use communication platforms to talk to their family members and friends. The Pew Research Center study and the study by Choi and DiNitto both show that digital literacy is very important, for adults.

3. Research Methodology

This study is about the security risks that come with browser autofill functions and how websites store information on your computer. The people who did this study wanted to see how autofill works and how it can be used to get information without permission. They made a website to test how autofill works and how it can be used to get information without people knowing. To do this they made a website using HTML, CSS and JavaScript to see how autofill works. They stored information in the browsers storage. Made the website fill in login fields automatically. They also made fields that could be filled in automatically without people knowing. They wanted to see how scripts could get information that was stored in the browser.

The people who did this study looked at the behavioral risks of autofill. They found that autofill can be used to get information without permission. They also found that people often do not know that autofill is filling in hidden fields. This can be a problem because people may think that only the fields they can see are being filled in. The study came up with some criteria to evaluate the risks of autofill. They looked at how sensitive information could be filled in without permission how long hidden fields could store information and how easily scripts could get information from autofill. They also looked at how different browsers handle autofill. The study found that autofill can be triggered by actions like clicking on a page or selecting a field. They also found that the layout of a website and the attributes of fields can affect how autofill works. They looked at how different browsers handle autofill. Found that there is no standard way of doing it. The study says that the way browsers handle autofill is not consistent. Some browsers are more aggressive in filling in fields while others are more careful. This can make it hard for developers to make websites. The study also says that third party scripts and bad website design can make vulnerabilities worse.

The study also looked at the factors involved in autofill risks. Many people do not know how autofill works and assume that it only fills in fields. This can create opportunities for attackers to get information without detection. The study says that we need to make sure that people are aware of how autofill works and that we need to have safeguards to protect sensitive information. The browser autofill functions are a problem because they can be used to get information without permission. The study says that we need to have standards, for how browsers handle autofill and that we need to make sure that people are aware of how it works. We also need to have safeguards to protect sensitive information.

The browser autofill functions need to be more secure. We need to make sure that people know how they work. Autofill functions can be used to get information without people knowing. The study found that this is a problem and that we need to do something about it. The browser autofill functions need to be more secure. We need to make sure that people are aware of how they work. We need to have safeguards to protect sensitive information and we need to make sure that developers are aware of the risks of autofill. The autofill functions are a problem. We need to fix them. Research methodology is the step-by-step process used to gather analyze and understand data to answer research questions and meet study goals.

In this study on literacy and cybersecurity awareness among senior citizens we used a structured approach to find out how much elderly individuals know about digital technology how they behave online and if they are aware of online risks. This study is a research study because it aims to describe and analyze digital literacy and cybersecurity awareness among senior citizens. Descriptive research helps identify patterns, behaviors and opinions about using technologies and online safety among older adults.

The research design lets us collect data from participants and look at their experiences with devices, internet use and cyber threats. We are focusing on literacy and cybersecurity awareness to understand how senior citizens use digital technology and stay safe online. The study helps us learn more about literacy and cybersecurity awareness among senior citizens.We want to know more about their experiences with devices and online safety practices. This will help us understand the level of knowledge and online behavior, among elderly individuals.

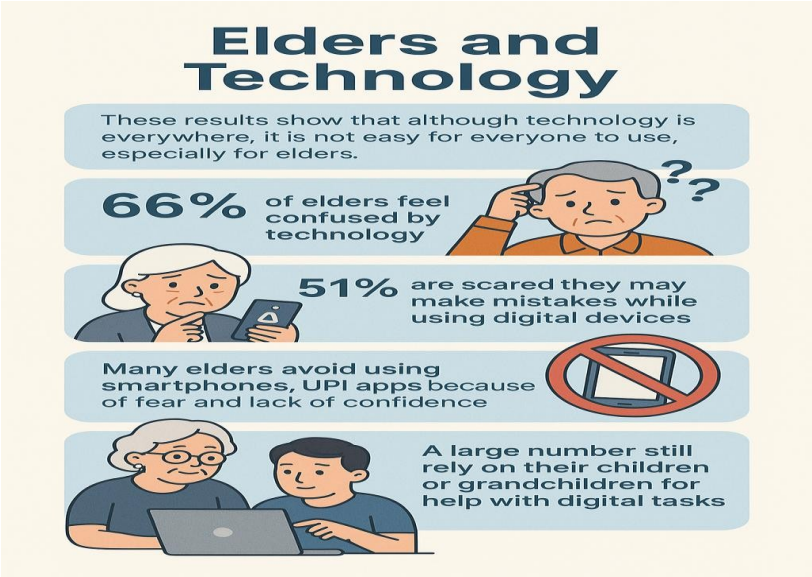

Fig. 2 Digital struggles of Senior Citizens.

4. Result

The study shows that senior citizens are getting better at using things but they still do not understand how to keep themselves safe online. Many senior citizens use things like smartphones and computers to do things like make phone calls send messages use social media and do their banking. However they do not know much about the things they can do with these devices and how to keep themselves safe. A lot of the people in the study said they learned how to use these things with the help of family and friends than taking a class.

The study also found out that while most senior citizens know about the internet and basic things they do not know much about the things that can happen online like fake emails, fake websites and people trying to steal their money. Many of the people in the study could not tell when something was suspicious like a link or a fake message. Some of the people in the study said they had been a victim of cyber fraud especially when they were using banking. This has made some senior citizens scared to use banking and other digital things.

The study also says that senior citizens are not using things as much as they could be because they are afraid of making mistakes and they do not feel confident. Some of the people in the study said they were worried about sharing their information or losing money because of a scam.. The people who had taken a class to learn about digital things were better at keeping themselves safe online like using strong passwords and being careful about the links they click on. Digital literacy is very important, for citizens and it can help them use digital things safely like digital literacy can help them use strong passwords and avoid bad links and digital literacy can help them understand how to use digital things safely.

The study tells us a lot about how good senior citizensre at using digital things and if they know about cybersecurity. The study looked at what senior citizens said in questionnaires and when they talked to people. It looked at how senior citizens use devices if they know about online dangers and if they can be safe online.

The study found out that a lot of citizens use digital devices, especially smartphones. Most of the people in the study said they use smartphones to talk to people send messages and use things like media or video calls to talk to their family. Some senior citizens use laptops or computers to look at the internet read news or use government services. This means that senior citizens are using things more and more but they do not use advanced digital tools very much.

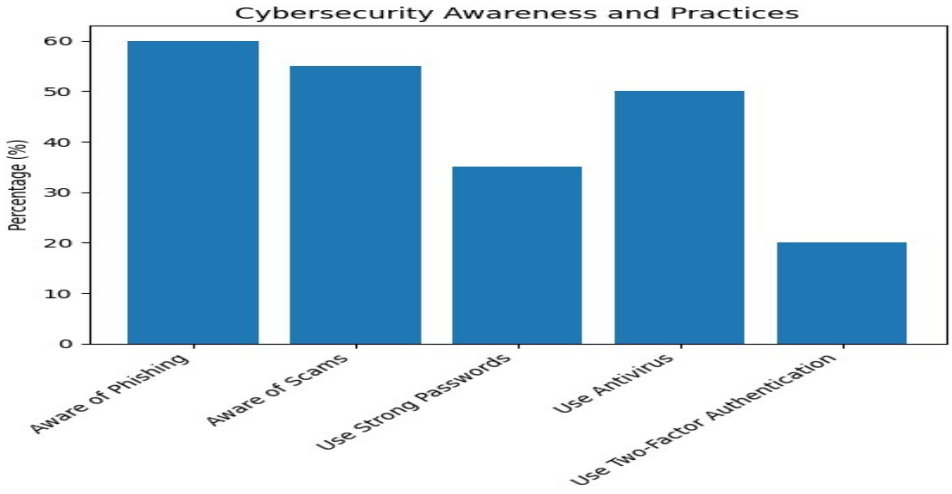

Fig. 3 Cybersecurity Awareness and Practices.

5. Conclusion

The findings of this research indicate that senior citizens are increasingly engaging with technologies compared to previous years. Many older adults now use smartphones and the internet as part of their routines mainly for communication and accessing information. However their digital skills generally remain limited to functions such as using smartphones sending and receiving emails browsing the internet and interacting on social media platforms. Senior citizens are participating in the environment but more complex digital tasks still present significant challenges. Operations such as banking, managing digital security settings installing applications or navigating advanced computer features often require a level of technical understanding that many older users have not yet developed.

As a result their interaction with technology tends to remain limited to activities that are easy to learn and repeat, like senior citizens using digital tools. Another important observation from the research is the lack of cybersecurity practices among many senior citizens. Although some participants are aware that online risks exist their overall security awareness remains relatively low. Many seniors do not regularly update their passwords enable security features or verify the authenticity of messages or links. This lack of precaution makes them particularly vulnerable to cyber threats, including phishing emails, fraudulent messages, financial scams and identity theft. Cybercriminals often target citizens because they may be less familiar with recognizing deceptive online behavior. The research also shows that several sociodemographic factors play a role in shaping digital literacy and cybersecurity behavior among senior citizen. Age, education level, exposure to technology and the availability of social or family support significantly influence how comfortably seniors use digital tools. Older participants, those aged 75 years and above generally showed lower levels of digital confidence and skill. Many individuals in this age group did not grow up with technologies and therefore had fewer opportunities to develop familiarity with computers or the internet earlier in life. In contrast seniors with levels of education or prior work experience involving technology tended to demonstrate better digital literacy and stronger awareness of online security practices. In addition family members younger relatives often play a supportive role by helping seniors navigate digital devices, install applications or resolve technical problems. Motivation also plays a role in encouraging older adults to use digital technologies. Many participants reported that their primary reasons for going include maintaining contact with family and friends accessing health-related information and purchasing products or services through online platforms. Social communication in particular has become a factor in reducing feelings of isolation among older adults. Despite these motivations several barriers continue to limit the participation of senior citizens in digital environments. One of the frequently mentioned challenges is the fear of making mistakes while using digital devices.

Many seniors worry that pressing the button or selecting the wrong option may cause problems such as losing important information or damaging the device. Rapid changes in technology interfaces also create difficulties as updates or redesigns of applications can make learned skills less useful. The findings of this research are consistent with theoretical frameworks that explain differences in technology access and adoption. Digital Divide Theory helps explain how unequal access to resources, knowledge and digital skills can create gaps between different groups of people. The Unified Theory of Acceptance and Use of Technology (UTAUT) provides insight into the factors that influence technology adoption among adults. Based on these findings the research emphasizes the importance of implementing targeted interventions that address the needs of senior citizens. Age-appropriate training programs designed with explanations, practical demonstrations and interactive learning methods can significantly improve both digital literacy and cybersecurity awareness. Technology companies also have a responsibility in creating digital environments that are easier for seniors to use.

Empowering individuals through digital literacy education and cybersecurity awareness programs can have significant benefits for both individuals and society. When seniors feel comfortable using technology they gain access, to information healthcare services, financial tools and social networks. This increased digital participation can improve their independence strengthen connections and enhance overall quality of life. At the time improved cybersecurity awareness helps protect them from online fraud and other digital risks protecting senior citizens. Video calls, messaging applications, and social networking platforms allow seniors to stay connected with relatives and friends, even when they live far away. At the same time, access to online healthcare information, appointment scheduling systems, and digital payment options has increased the practical value of digital tools for everyday life.

Despite these motivations, several barriers continue to limit the full participation of senior citizens in digital environments. One of the most frequently mentioned challenges is the fear of making mistakes while using digital devices. Many seniors worry that pressing the wrong button or selecting the wrong option may cause problems such as losing important information or damaging the device. Rapid changes in technology interfaces also create difficulties, as updates or redesigns of applications can make previously learned skills less useful. Additionally, technical terminology and complicated instructions can be confusing for individuals who do not have a technical background. As a result, many seniors rely heavily on assistance from family members, friends, or community support programs when using digital tools.

The findings of this research are consistent with several theoretical frameworks that explain differences in technology access and adoption. Digital Divide Theory helps explain how unequal access to technological resources, knowledge, and digital skills can create gaps between different groups of people. In the context of this study, the digital divide appears not only in terms of access to technology but also in the ability to use it safely and effectively. Some seniors may have access to devices and internet connections but still lack the necessary knowledge to protect themselves from online risks. Similarly, the Unified Theory of Acceptance and Use of Technology (UTAUT) provides insight into the factors that influence technology adoption among older adults. According to this framework, elements such as performance expectancy, effort expectancy, and social influence affect how individuals decide to adopt and continue using technology. For many seniors, technology becomes more appealing when it clearly

improves daily activities and when the effort required to learn it is manageable.

Based on these findings, the research emphasizes the importance of implementing targeted interventions that address the specific needs of senior citizens. Age-appropriate training programs designed with simple explanations, practical demonstrations, and interactive learning methods can significantly improve both digital literacy and cybersecurity awareness. Community centers, libraries, and educational institutions can play an important role in providing training sessions that help seniors build confidence in using digital devices. In addition, government agencies and non-profit organizations can support digital inclusion initiatives that focus on older populations.

Technology companies also have an important responsibility in creating digital environments that are easier for seniors to use. Designing age-friendly interfaces, using clear instructions, providing larger text options, and simplifying navigation can greatly improve accessibility for older users. Public awareness campaigns about cybersecurity risks should also be developed in ways that are easy for seniors to understand. When these efforts are combined with continuous support systems, seniors are more likely to develop confidence in their digital abilities and become active participants in online environments.

Reference

[1] Bhatia, R., & Khan, F. (2024). Digital Literacy Among Elderly People and Usage of Digital Means. International Journal of Research and Analysis in Commerce and Management. Link: Read the article

[2] Gupta, P. (2025). Understanding Cybersecurity Awareness and Perceptions Among Older Adults in India. Scientific and Practical Cyber Security Journal. Link: View the research paper

[3] Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2021). Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective. Journal of Computer Information Systems. Link: https://doi.org/10.1080/08874417.2019.1579076

[4] Upadhyay, R., Martolia, M., & Singh, S. (2025). Digital Literacy and Online Safety Among Senior Citizens: An Evaluation of the Sach Ke Sathi. Journal of Informatics Education and Research. Link: Open the journal article

[5] Pawlicka, A., Tomaszewska, R., Krause, E., & Choraś, M. (2023). Has the Pandemic Made Us More Digitally Literate? Journal of Ambient Intelligence and Humanized Computing. Link: Access the article

[6] Ozkan-Ozen, Y., & Kazancoglu, Y. (2022). A Systematic Review on Digital Literacy. Smart Learning Environments. Link: Read the systematic review

[7] Burton, J., Nicholson, J., & McGlasson, C. (2025). Cybercrime Against Senior Citizens. Security Journal (Springer). Link: https://link.springer.com/article/10.1057/s41284-025-00482-4

[8] Huang, L.-S., Chen, E., Barth, A., Rescorla, E., & Jackson, C. "Talking to Yourself for Fun and Profit. IEEE Symposium on Security and Privacy", (2012), 140–154.

[9] Calzavara, S., Rabitti, A., Bugliesi, M., & Zannone, N. "Content Security Problems? Evaluating the Effectiveness of Content Security Policy", (2015). *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 1360–1373.

[10] Stock, B., Lekies, S., Mueller, T., Spiegel, P., & Johns, M. "Precise Client-Side Protection Against DOMBased Cross-Site Scripting", (2014). USENIX Security Symposium, 655–670.

[11] Reis, C., Dunagan, J., Wang, H. J., Dubrovsky, O., & Esmeir, S. "BrowserShield: Vulnerability-Driven Filtering of Dynamic HTML. ACM Transactions on the Web", (2006), 1(3), 1–37.

[12] Lekies, S., Johns, M., & Stock, B. "Clickjacking: Attacks and Defences". Proceedings of the USENIX Security Symposium, (2012), 413–428.

[13] Barth, A., Jackson, C., & Mitchell, J. C. "Robust Defences for Cross-Site Request Forgery", (2008). Proceedings of the ACM Conference on Computer and Communications Security (CCS), 75–88.

[14] Stamm, S., Sterne, B., & Markham, G. "Reining in the Web with Content Security Policy", (2010). Proceedings of the International World Wide Web Conference (WWW), 921–930.

[15] Rossow, G., Dietrich, C. J., Bos, H., Cavallaro, L., Van Steen, M., Freiling, F. C., & Pohlmann, N. "Prudent Practices for Designing Malware Detectors", (2012). IEEE Symposium on Security and Privacy, 165–179.

[16] Bortz, A., Barth, A., & Czeskis, A. "Origin Cookies: Session Integrity for Web Applications", (2011). Proceedings of the IEEE Web 2.0 Security and Privacy Workshop. (2012)