ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep709

Designing Age-Inclusive Cybersecurity: Enhancing Protection for Older Adults in Digital Environments

Seth Nti Berko[1]; Loveth A. Odozor[2]

[1]Information Security Analyst SSBiz Solutions, Georgia Atlanta.
[2]MSC Cybersecurity, Katz School of Science and Health, Yeshiva University.

Publication Date: 2025/09/26

Abstract: As digital technology becomes increasingly integral to daily life, older adults face unique cybersecurity challenges that require specialized attention and innovative solutions. This comprehensive review examines the intersection of aging and cybersecurity, exploring how age-related changes in cognition, technology adoption patterns, and digital literacy impact vulnerability to cyber threats. Through analysis of recent research spanning 2010-2025, this article identifies critical gaps in current cybersecurity approaches and proposes age-inclusive design principles that enhance protection for older adults while maintaining usability and autonomy. The findings reveal that traditional cybersecurity measures often fail to account for the diverse needs, capabilities, and preferences of older users, necessitating a paradigm shift toward more inclusive and adaptive security frameworks. Key recommendations include developing age-appropriate training programs, implementing intuitive security interfaces, and creating community-based support systems that leverage collective efficacy in cybersecurity practices.

Keywords: *Age-Inclusive Design, Cybersecurity, Older Adults, Digital Literacy, Human Factors, Security Usability*.

How to Cite: Seth Nti Berko; Loveth A. Odozor (2025) Designing Age-Inclusive Cybersecurity: Enhancing Protection for Older Adults in Digital Environments. *International Journal of Innovative Science and Research Technology*, 10(9), 1616-1628. https://doi.org/10.38124/ijisrt/25sep709

I. INTRODUCTION

The rapid digitization of essential services and social interactions has fundamentally transformed how individuals engage with technology across all age groups. For older adults, this digital transformation presents both unprecedented opportunities for connection and independence, as well as significant cybersecurity challenges that require careful consideration and innovative solutions. Morrison, Nicholson, Coventry, and Briggs (2023) emphasize the importance of recognizing diversity in older adults' cybersecurity needs, challenging the notion that this demographic represents a homogeneous group with uniform technological capabilities and security requirements.

The post-pandemic era has accelerated digital adoption among older adults, with many experiencing their first sustained engagement with online platforms, digital health monitoring systems, and remote communication technologies. Pacheco (2024) explored older adults' safety and security attitudes following this period of increased digital engagement, revealing complex relationships between technology adoption, perceived benefits, and security concerns. This shift has highlighted the urgent need for cybersecurity frameworks that accommodate the unique characteristics, preferences, and limitations of older adult users while avoiding patronizing or overly restrictive approaches.

Traditional cybersecurity paradigms have predominantly been designed with younger, more technologically proficient users in mind, often resulting in security measures that create barriers rather than protection for older adults. Morrison, Coventry, and Briggs (2021) investigated how older adults feel about engaging with cybersecurity, uncovering significant emotional and practical barriers that prevent effective security behavior adoption. These findings suggest that age-inclusive cybersecurity design must address not only technical vulnerabilities but also the psychological and social factors that influence older adults' security decision-making processes.

The significance of this research extends beyond individual user protection to encompass broader societal implications. As the global population ages and digital dependency increases, the cybersecurity vulnerability of older adults represents a growing concern for families, healthcare systems, financial institutions, and digital service providers. Understanding and addressing these vulnerabilities through age-inclusive design principles is essential for

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep709

creating a more secure and equitable digital environment for all users.

II. LITERATURE REVIEW

➢ *Age-Related Cybersecurity Vulnerabilities*

Research consistently demonstrates that older adults face distinct cybersecurity challenges that stem from both age-related changes and the design of existing security systems. Morrison, Coventry, and Briggs (2020) examined technological change during the retirement transition, identifying how major life changes can increase cybersecurity vulnerability through disrupted routines, increased online activity, and reduced technical support networks. This transitional period often coincides with increased exposure to online services for healthcare, financial management, and social connection, creating a perfect storm of heightened risk and reduced protective factors.

Age-related cognitive changes play a significant role in cybersecurity vulnerability, particularly in areas such as working memory, processing speed, and inhibitory control. Grilli et al. (2021) conducted a comprehensive study examining older adults' ability to discriminate between safe and malicious emails, finding that advancing age was associated with greater difficulty in identifying phishing attempts. Their research revealed that older adults were more likely to focus on superficial email characteristics rather than critically evaluating sender authenticity and content credibility, suggesting that age-related changes in cognitive processing may increase susceptibility to social engineering attacks.

The relationship between aging and technology proficiency further compounds cybersecurity vulnerabilities. Nicholson, Coventry, and Briggs (2013) investigated age-related performance issues for authentication systems, finding that older adults experienced significantly greater difficulty with both PIN-based and biometric authentication methods. These performance challenges often lead to work around behaviors that compromise security, such as writing down passwords, using simple authentication methods, or avoiding security features altogether.

Ebner et al. (2020) conducted groundbreaking research uncovering susceptibility risk to online deception in aging, revealing that certain personality traits and cognitive characteristics may predispose older adults to falling victim to cybercrime. Their findings suggest that factors such as reduced skepticism, increased trust in authority figures, and changes in risk perception contribute to heightened vulnerability to various forms of online deception.

➢ *Information Seeking and Security Awareness*

The ways in which older adults seek and process cybersecurity information differ significantly from younger users, with important implications for security education and awareness campaigns. Nicholson, Coventry, and Briggs (2019) explored cybersecurity information seeking behaviors among older adults, discovering that many relied on traditional media sources and trusted personal networks rather than official cybersecurity resources. Their research revealed that older adults often applied a "headline mentality" to cybersecurity information, believing that truly important security threats would be prominently featured in mainstream news coverage.

This information-seeking pattern creates vulnerabilities because cybersecurity threats often evolve rapidly and may not receive widespread media attention until significant damage has occurred. Furthermore, the technical language and complex instructions commonly found in cybersecurity guidance can be particularly challenging for older adults who may lack the technical vocabulary or conceptual frameworks necessary to understand and implement security recommendations.

Blackwood-Brown, Levy, and D'Arcy (2021) examined cybersecurity awareness and skills from a motivation perspective, finding that older adults' security behaviors were strongly influenced by perceived relevance, self-efficacy beliefs, and social norms within their peer groups. Their research highlighted the importance of designing cybersecurity education that connects to older adults lived experiences and addresses their specific concerns and priorities.

➢ *Gender and Individual Differences*

Cybersecurity vulnerability among older adults is further complicated by gender differences and individual variation in technology adoption and security practices. Branley-Bell, Coventry, Dixon, Joinson, and Briggs (2021) explored age and gender differences in cybersecurity behavior, revealing complex interactions between demographic factors and security practices. Their findings indicated that older women were more likely to seek help with cybersecurity issues but also more likely to express anxiety about technology use, while older men were more likely to overestimate their cybersecurity knowledge and engage in risky online behaviors.

These gender differences have important implications for cybersecurity design and education, suggesting that effective interventions must account for diverse learning styles, communication preferences, and support-seeking behaviors within the older adult population. Cross (2017) examined seniors' attitudes toward identity crime, finding that many older adults had limited understanding of how personal information could be misused and often underestimated the value of seemingly innocuous data such as driver's license numbers.

➢ *Technology-Specific Vulnerabilities*

As older adults increasingly adopt mobile devices and smart home technologies, new categories of cybersecurity vulnerabilities emerge that require specialized attention. Chen et al. (2025) conducted extensive research on older adults' perceptions, barriers, and coping strategies related to Internet of Things (IoT) privacy and security in health monitoring contexts. Their findings revealed that while older adults appreciated the health benefits of connected devices,

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep709

they struggled to understand and manage the privacy implications of continuous data collection and sharing.

Ray, Wolf, Kuber, and Aviv (2021) investigated why older adults often avoid password managers despite their security benefits, identifying usability barriers, trust concerns, and conceptual difficulties that prevent adoption of these important security tools. Their research highlighted how well-intentioned security technologies can become accessibility barriers when not designed with older adult users' needs and preferences in mind.

The adoption of smart home technologies presents particular challenges for older adults, who must balance the benefits of automation and safety monitoring with concerns about privacy and security. Tural, Lu, and Cole (2021) examined older adults' attitudes toward smart home technologies, finding that security concerns were among the primary barriers to adoption, along with cost and complexity issues.

Table 1 Summary of Age-Related Cybersecurity Challenges and Contributing Factors

Challenge Category	Specific Issues	Contributing Factors	Research Source
Cognitive Processing	Difficulty identifying phishing emails	Age-related changes in working memory, processing speed	Grilli et al. (2021)
Authentication	Problems with PIN and biometric systems	Motor difficulties, memory issues, technology anxiety	Nicholson et al. (2013)
Information Seeking	Reliance on mainstream media for security info	Limited technical vocabulary, trust in traditional sources	Nicholson et al. (2019)
Technology Adoption	Avoidance of password managers	Usability barriers, trust concerns, complexity	Ray et al. (2021)
Social Engineering	Increased susceptibility to online deception	Reduced skepticism, trust in authority, risk perception changes	Ebner et al. (2020)
IoT Devices	Privacy concerns with health monitoring	Limited understanding of data sharing, trust issues	Chen et al. (2025)

➢ *Cybersecurity Training and Education Approaches*

- *Current Training Methodologies*

The development of effective cybersecurity training for older adults requires careful consideration of age-related learning preferences, cognitive changes, and motivational factors. Prümmer, van Steen, and van den Berg (2024) conducted a systematic review of current cybersecurity training methods, identifying significant gaps in age-appropriate educational approaches. Their analysis revealed that most existing training programs were designed with younger users in mind and failed to account for older adults' unique learning needs and preferences.

Traditional cybersecurity training often relies heavily on technical explanations, abstract concepts, and fear-based messaging that can be counterproductive for older adult learners. Al-Daeef, Basir, and Saudi (2017) reviewed security awareness training approaches, finding that effective programs for older adults required concrete examples, hands-on practice opportunities, and positive reinforcement rather than intimidation tactics.

Fujs, Mihelič, and Vrhovec (2025) developed an innovative smart information and cyber security training approach specifically designed for older adults, incorporating adaptive learning technologies and personalized content delivery. Their SmartICST system demonstrated promising results in improving both cybersecurity knowledge and confidence among older adult participants, suggesting that technology-enhanced learning can be effective when properly designed for this population.

- *Competence Assessment and Development*

Understanding older adults' existing cybersecurity competencies is essential for developing targeted and effective training interventions. Mihelič, Vrhovec, and Fujs (2024) examined the cybersecurity competence of older adult mobile device users, identifying significant variation in both knowledge and skills within this population. Their research highlighted the importance of individualized assessment and training approaches that build upon existing strengths while addressing specific knowledge gaps.

The assessment of digital competence among older adults requires tools that are both accurate and age-appropriate. Roque and Boot (2018) developed the Mobile Device Proficiency Questionnaire specifically for older adults, providing a validated instrument for measuring technology skills that relate directly to cybersecurity capabilities. Their work demonstrated that accurate assessment of baseline competencies is crucial for designing effective training programs.

Loi, Iversen, and Røed (2019) investigated the effectiveness of different message formats for cybersecurity awareness, finding that tweet-length messages could be effective for older adults when properly designed. Their research suggested that brief, focused educational content might be more effective than lengthy training sessions for maintaining ongoing security awareness.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep709

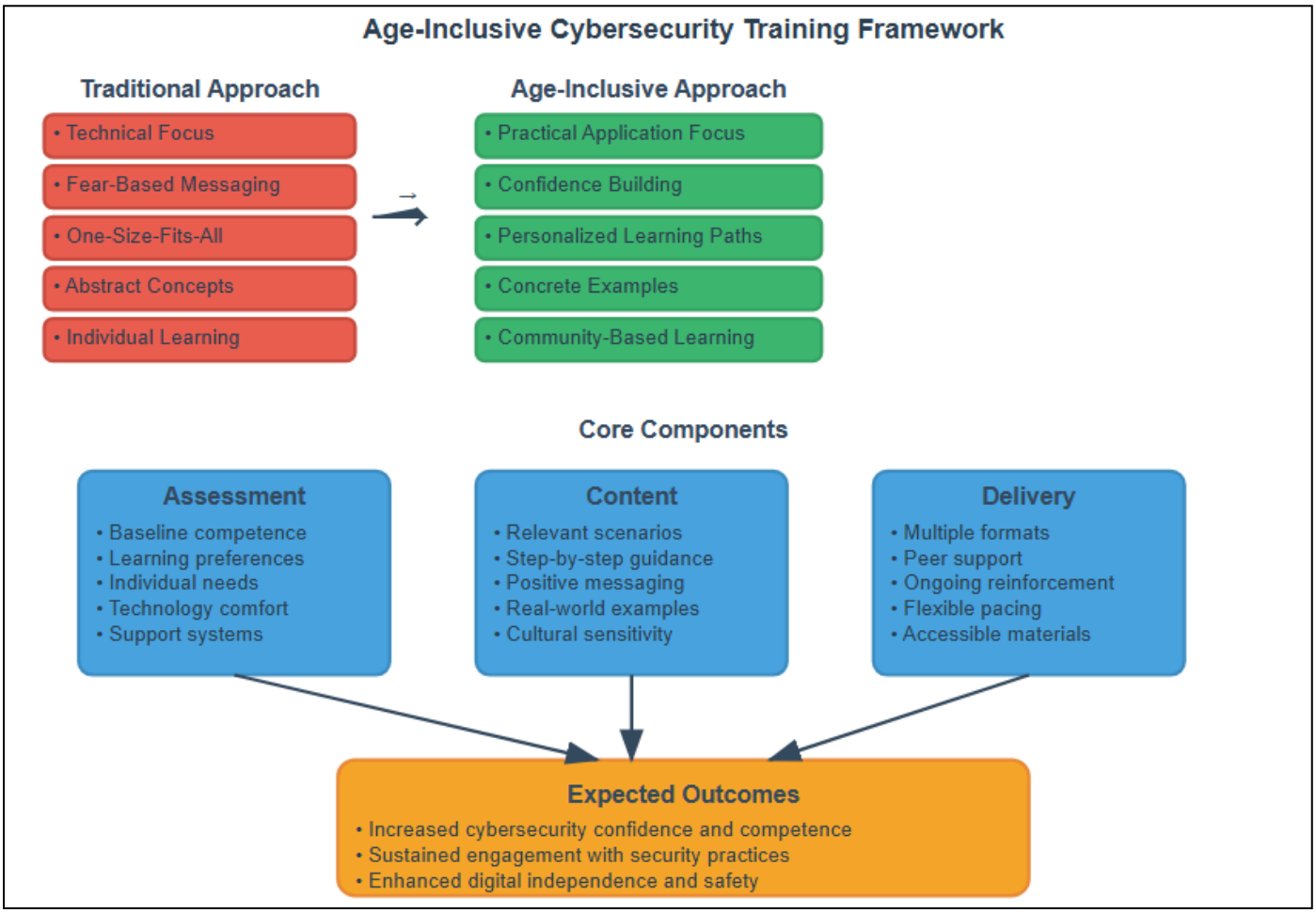

Fig 1 Age-Inclusive Cybersecurity Training Framework

➢ *Technology Design and Usability Considerations*

- *Authentication and Access Control*

The design of authentication systems represents a critical intersection between security and accessibility for older adult users. Carstens, McCauley-Bell, Malone, and DeMara (2004) evaluated the human impact of password authentication practices, identifying significant usability challenges that disproportionately affected older users. Their research demonstrated that complex password requirements often led to insecure workaround behaviors, suggesting that security policies must balance protection with practicality.

The challenge of authentication design for older adults extends beyond traditional password systems to encompass biometric and multi-factor authentication approaches. While these technologies offer potential security benefits, they also present unique usability challenges for older users who may experience age-related changes in fine motor control, vision, or cognitive processing speed.

Jeske, Briggs, and Coventry (2016) explored the relationship between impulsivity and decision-making on mobile devices, finding that older adults often made more deliberate but potentially less secure choices when faced with authentication prompts. Their research highlighted the importance of designing authentication interfaces that support careful decision-making without creating excessive cognitive burden.

- *Smart Home and IoT Security*

The proliferation of smart home technologies presents both opportunities and challenges for older adult cybersecurity. Chhetri and Motti (2021) identified vulnerabilities in security and privacy of smart home devices, finding that many systems failed to provide adequate user control over privacy settings or clear information about data collection and sharing practices.

Percy Campbell, Yu, Duggan, Mentis, and Thapa (2024) conducted a scoping review of user perceptions of smart home surveillance among adults aged 50 and older, revealing complex attitudes toward privacy and security in domestic technology environments. Their findings indicated that older adults valued the safety and convenience benefits of smart home systems but were concerned about data privacy and the potential for surveillance by unauthorized parties.

The design of IoT security interfaces for older adults requires particular attention to information presentation, control accessibility, and trust-building features. Many current systems present security and privacy information in technical language that may be difficult for older adults to understand and act upon effectively.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep709

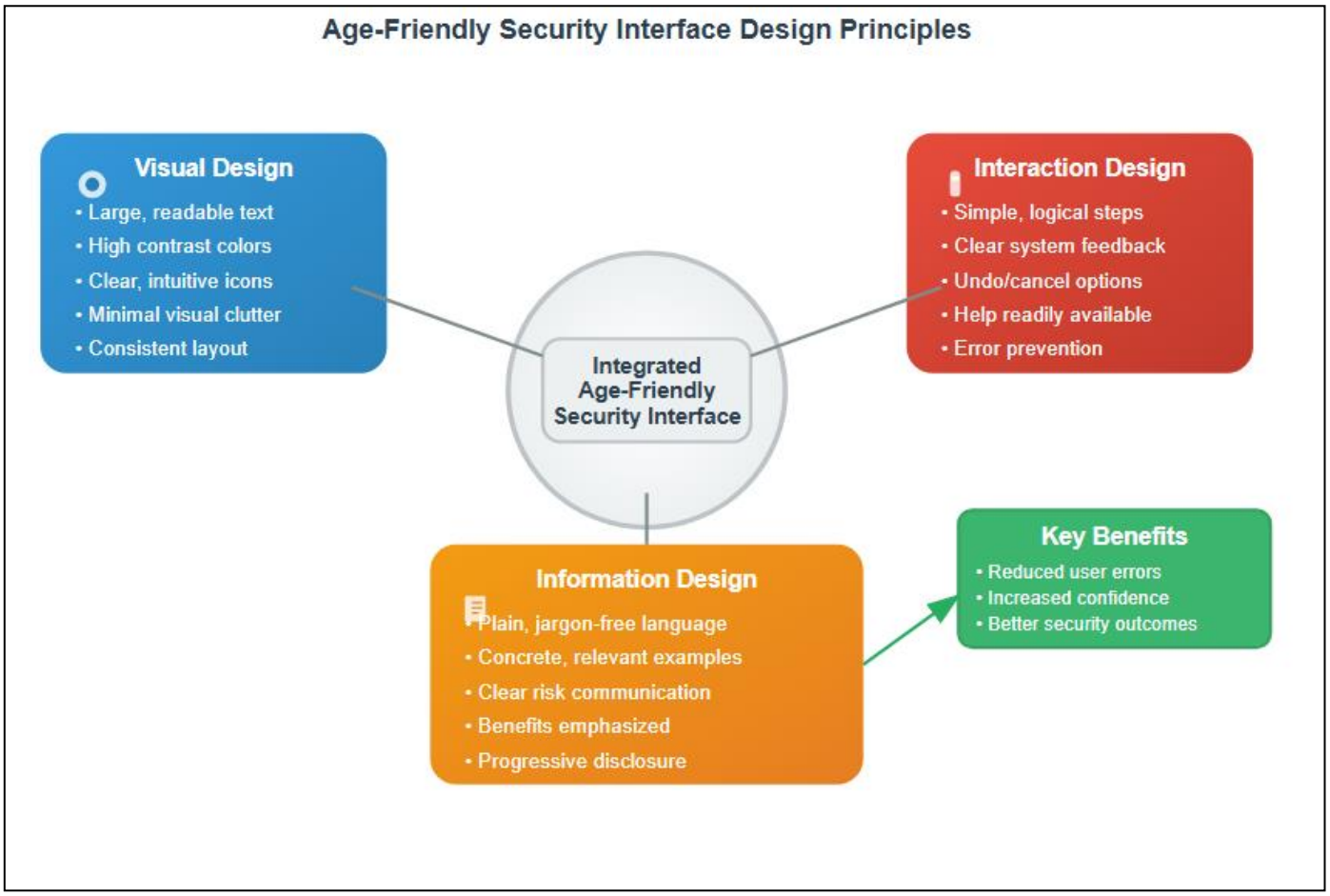

Fig 2 Age-Friendly Security Interface Design Principles

➢ *Community and Social Approaches to Cybersecurity*

- *Collective Efficacy and Peer Support*

The social dimensions of cybersecurity are particularly important for older adults, who often rely on family members, friends, and community networks for technology support and guidance. Kropczynski, Linehan, Nir, Wisniewski, and Carroll (2021) explored the concept of building community collective efficacy for managing digital privacy and security within older adult communities. Their research demonstrated that peer-to-peer learning and mutual support could be highly effective for improving cybersecurity practices among older adults.

Community-based approaches to cybersecurity education offer several advantages for older adult learners, including familiar social contexts, peer validation, and opportunities for hands-on practice with trusted supporters. These approaches can help address the social isolation that may increase cybersecurity vulnerability by connecting older adults with peers who share similar experiences and challenges.

Shillair et al. (2015) investigated online safety education approaches, finding that convincing Internet users to protect themselves required addressing both individual knowledge gaps and social norms around security behavior. Their research highlighted the importance of creating supportive environments where older adults feel comfortable asking questions and admitting uncertainty about cybersecurity practices.

- *Family and Intergenerational Support*

The role of family members in older adults' cybersecurity practices presents both opportunities and challenges for age-inclusive security design. While younger family members often serve as informal technology support providers, this relationship can sometimes lead to paternalistic approaches that reduce older adults' autonomy and confidence in managing their own cybersecurity.

Effective intergenerational cybersecurity support requires balancing assistance with empowerment, providing older adults with the knowledge and tools they need to make informed security decisions while maintaining appropriate backup support when needed. This approach requires careful consideration of communication strategies, respect for older adults' preferences and priorities, and recognition of their existing knowledge and capabilities.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep709

Table 2 Community-Based Cybersecurity Support Models

Support Model	Key Features	Advantages	Challenges	Implementation Considerations
Peer Learning Groups	Older adults learning together	Reduced anxiety, shared experiences	Varying skill levels	Need trained facilitators
Intergenerational Programs	Younger and older adults paired	Technology expertise sharing	Potential power imbalances	Respect for autonomy essential
Community Centers	Centralized support location	Familiar environment, ongoing access	Limited reach, resource intensive	Integration with existing services
Digital Volunteers	Trained community volunteers	Personalized assistance, trust	Volunteer recruitment/retention	Background checks, training
Online Communities	Virtual peer support networks	Accessible, broad reach	Digital divide issues	Moderation, safety protocols

➢ *Vulnerability Assessment and Risk Factors*

- *Cognitive and Psychological Factors*

Understanding the cognitive and psychological factors that contribute to cybersecurity vulnerability among older adults is essential for developing effective protective interventions. Button, Nicholls, Kerr, and Owen (2014) examined why individuals fall victim to online frauds, identifying cognitive biases and emotional states that increase susceptibility to cybercrime. Their research revealed that factors such as social isolation, financial stress, and health concerns could create conditions that made older adults more vulnerable to social engineering attacks.

The relationship between cognitive aging and cybersecurity vulnerability is complex and multifaceted. While some age-related changes may increase risk, older adults also possess valuable life experience and wisdom that can serve as protective factors when properly leveraged. Mentis, Madjaroff, and Massey (2019) explored cybersecurity risks and benefits for older adults with mild cognitive impairment, finding that appropriate support and simplified interfaces could enable safe technology use even among individuals with cognitive challenges.

Whitty and Buchanan (2012) investigated online romance scams, a type of cybercrime that disproportionately affects older adults, particularly women. Their research highlighted how social engineering tactics exploit universal human needs for connection and companionship, suggesting that effective protection requires addressing both technical vulnerabilities and social-emotional factors.

- *Behavioral and Decision-Making Patterns*

The decision-making processes that older adults use when encountering potential cybersecurity threats differ significantly from those of younger users. Grimes, Hough, Mazur, and Signorella (2010) examined older adults' knowledge of internet hazards, finding that many had limited awareness of common online threats and tended to rely on intuitive rather than analytical decision-making strategies when evaluating online risks.

Chakraborty et al. (2016) investigated online shopping intentions following data breaches, comparing older and younger adults' responses to security incidents. Their findings revealed that older adults were more likely to discontinue online shopping entirely following a security breach, suggesting that negative security experiences can have lasting impacts on technology adoption and use patterns among older users.

The tendency for older adults to make more cautious decisions can be both protective and problematic in cybersecurity contexts. While caution may prevent some risky behaviors, it can also lead to avoidance of beneficial technologies or excessive reliance on others for technology management, potentially creating new vulnerabilities.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep709

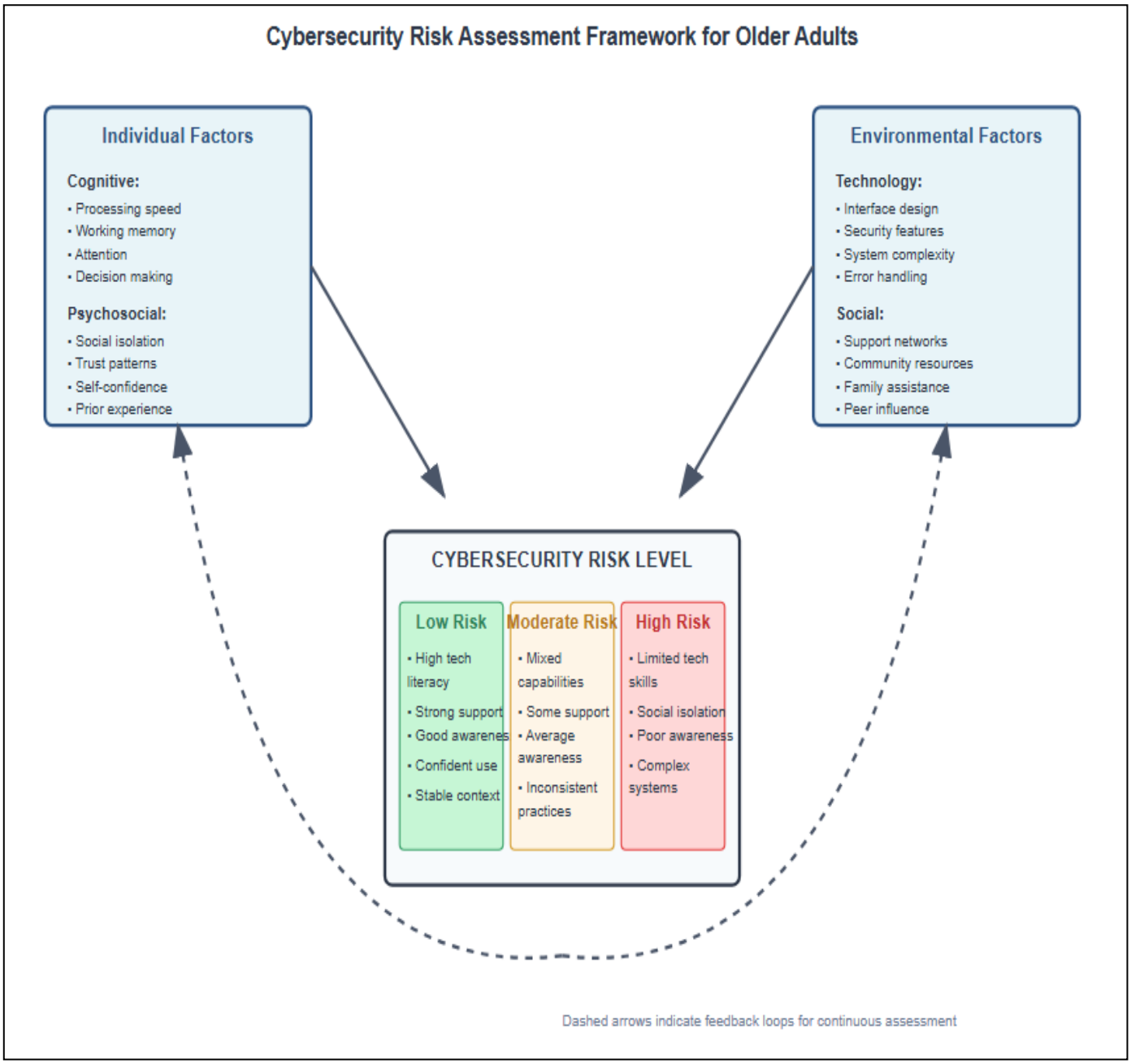

Fig 3 Cybersecurity Risk Assessment Framework for Older Adults

➢ *Emerging Technologies and Future Considerations*

- *Artificial Intelligence and Adaptive Security*

The integration of artificial intelligence and machine learning technologies into cybersecurity systems offers promising opportunities for creating more adaptive and personalized protection for older adults. Aletras, Karyotis, Tsagkias, Aroyo, and Moens (2021) proposed leveraging human factors in cybersecurity through integrated methodological approaches, suggesting that AI systems could potentially adapt to individual users' capabilities, preferences, and behavioral patterns.

Adaptive security systems could address many of the challenges that older adults face with traditional cybersecurity tools by automatically adjusting interface complexity, providing contextual guidance, and learning from user behavior to improve protection over time. However, the development of such systems requires careful consideration of privacy implications, user control, and the potential for creating new forms of technological dependency.

The use of AI in cybersecurity for older adults also raises important questions about transparency, explainability, and trust. Older adults may be particularly concerned about automated decision-making systems that they do not understand or cannot control, suggesting that AI-enhanced security tools must provide clear explanations and maintain user agency.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep709

- *Health Technology Integration*

The increasing integration of health monitoring and management technologies into older adults' daily lives creates new cybersecurity challenges and opportunities. The sensitive nature of health data, combined with the critical importance of reliable access to health technologies, requires specialized approaches to security that balance protection with accessibility and usability.

Connected health devices, telemedicine platforms, and digital health records systems must be designed to provide robust security without creating barriers to essential healthcare access. This requires close collaboration between cybersecurity professionals, healthcare providers, and older adult users to develop solutions that meet real-world needs and constraints.

Table 3 Emerging Technology Impacts on Older Adult Cybersecurity

Technology Domain	Opportunities	Challenges	Design Considerations
AI-Powered Security	Adaptive interfaces, personalized protection	Complexity, trust, privacy	Explainable AI, user control
Voice Assistants	Natural interaction, accessibility	Privacy, authentication	Clear privacy controls
Biometric Systems	Convenience, security	Age-related changes	Multiple modalities
IoT Health Devices	Health monitoring, emergency response	Data privacy, security	Clear consent processes
Augmented Reality	Enhanced security information	Cognitive overload	Simple, contextual displays
Blockchain	Secure transactions, identity protection	Technical complexity	Simplified interfaces

➢ *Age-Inclusive Design Recommendations*

- *Universal Design Principles*

The application of universal design principles to cybersecurity represents a fundamental shift from accommodation-based approaches to inclusive design that benefits users of all ages and abilities. Nägle and Schmidt (2012) examined computer acceptance among older adults, identifying key factors that influence technology adoption and continued use. Their findings suggest that cybersecurity systems designed with universal principles in mind are more likely to be accepted and effectively used by older adult populations.

Universal design in cybersecurity encompasses several key principles including simplicity and intuitive use, tolerance for error, low physical effort, and perceptible information. These principles can guide the development of security interfaces that are accessible to users with varying levels of technical expertise, cognitive abilities, and sensory capabilities.

The implementation of universal design principles requires moving beyond traditional security paradigms that prioritize technical sophistication over usability. Instead, effective age-inclusive cybersecurity systems must balance robust protection with intuitive interfaces that support successful security behavior adoption across diverse user populations.

- *Personalization and Adaptability*

Effective age-inclusive cybersecurity design must accommodate the significant diversity that exists within the older adult population. Personalization features that allow users to adjust interface complexity, information presentation, and interaction methods can help ensure that security systems meet individual needs and preferences while maintaining appropriate protection levels.

Adaptive systems that learn from user behavior and adjust their operation accordingly offer particular promise for older adult cybersecurity. Such systems could potentially reduce cognitive burden by automating routine security tasks while providing guidance and support for more complex security decisions.

The development of personalized cybersecurity systems requires careful attention to privacy protection and user control. Older adults must understand what information is being collected about their behavior and have meaningful control over how this information is used to adapt system operation.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep709

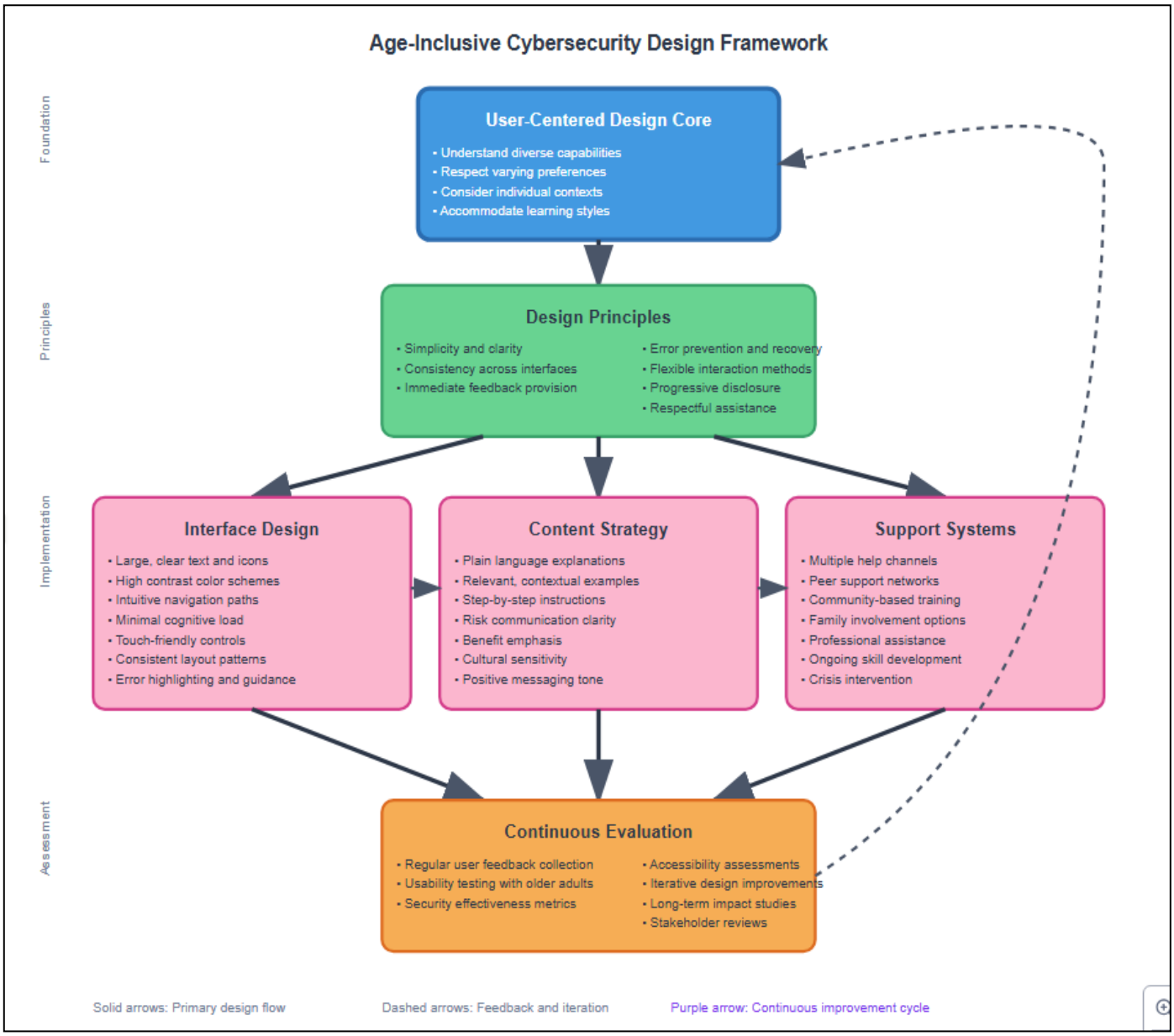

Fig 4 Age-Inclusive Cybersecurity Design Framework

➢ *Implementation Strategies and Best Practices*

- *Stakeholder Collaboration*

Successful implementation of age-inclusive cybersecurity requires collaboration among multiple stakeholders including technology developers, cybersecurity professionals, healthcare providers, community organizations, and older adult users themselves. Coventry, Briggs, Jeske, and van Moorsel (2014) proposed a structured approach to creating cybersecurity behavioral interventions that emphasizes the importance of understanding user contexts and involving target populations in the design process.

Effective stakeholder collaboration requires recognizing and respecting the expertise that different groups bring to the cybersecurity challenge. Older adult users possess valuable insights about their own needs, preferences, and constraints that are essential for developing effective solutions. Healthcare providers understand the health-related factors that may influence cybersecurity behavior, while community organizations can provide access to target populations and implementation venues.

Technology developers and cybersecurity professionals must be willing to challenge traditional assumptions about security design and embrace approaches that prioritize usability and accessibility alongside protection. This may require significant changes to development processes, evaluation criteria, and success metrics.

- *Evaluation and Measurement*

The evaluation of age-inclusive cybersecurity interventions requires comprehensive assessment approaches that consider both objective security outcomes and subjective user experiences. Traditional cybersecurity metrics such as vulnerability detection rates or security incident frequency

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep709

may not fully capture the effectiveness of interventions designed for older adult populations.

Evaluation frameworks for age-inclusive cybersecurity should incorporate measures of user confidence, technology adoption, independence maintenance, and quality of life impacts in addition to traditional security metrics. These broader outcome measures are essential for understanding whether cybersecurity interventions genuinely improve older adults' digital experiences or create new barriers and challenges.

Longitudinal evaluation approaches are particularly important for understanding how older adults' cybersecurity needs and capabilities change over time, allowing for iterative improvement of interventions and adaptation to evolving threat landscapes and technology environments.

Table 4 Implementation Timeline and Milestones for Age-Inclusive Cybersecurity Programs

Phase	Duration	Key Activities	Success Metrics	Stakeholders
Planning	3-6 months	Stakeholder engagement, needs assessment, resource allocation	Stakeholder buy-in, clear objectives	All stakeholders
Design	6-12 months	User research, prototype development, initial testing	Usable prototypes, positive user feedback	Designers, users, researchers
Pilot Implementation	6-9 months	Small-scale deployment, intensive evaluation	Improved security behaviors, user satisfaction	Community partners, users
Refinement	3-6 months	System improvements, training updates	Enhanced usability, reduced support needs	Technical teams, trainers
Full Deployment	12+ months	Broad implementation, ongoing support	Widespread adoption, sustained behavior change	All stakeholders
Evaluation & Iteration	Ongoing	Continuous monitoring, periodic updates	Maintained effectiveness, user retention	Researchers, support staff

III. FUTURE RESEARCH DIRECTIONS

➢ *Longitudinal Studies and Aging Trajectories*

Future research in age-inclusive cybersecurity must adopt longitudinal approaches that track how older adults' cybersecurity needs, capabilities, and vulnerabilities change over time. Current research primarily provides cross-sectional snapshots that may not fully capture the dynamic nature of aging and technology interaction. Understanding how cybersecurity challenges evolve as individuals age, experience health changes, or encounter major life transitions is essential for developing adaptive and sustainable protection strategies.

Longitudinal research should also examine how cohort effects influence cybersecurity attitudes and behaviors. Current older adult populations include individuals who experienced the digital revolution as adults, while future older adult cohorts will have grown up with digital technologies. These generational differences may significantly impact cybersecurity approaches and intervention effectiveness.

Research examining the intersection of cognitive aging and cybersecurity over time could provide valuable insights into when and how to adapt security systems to accommodate age-related changes. This research should consider both normative aging processes and pathological changes associated with conditions such as dementia or mild cognitive impairment.

➢ *Cross-Cultural and Global Perspectives*

Most existing research on older adults and cybersecurity has been conducted in Western, developed countries, limiting the generalizability of findings to diverse global populations. Future research must examine how cultural factors, economic conditions, digital infrastructure differences, and varying social support systems influence older adults' cybersecurity experiences across different international contexts.

Cross-cultural research could reveal important insights about the role of family structures, community support systems, and cultural attitudes toward technology and aging in shaping cybersecurity practices. Understanding these cultural variations is essential for developing cybersecurity approaches that can be effectively adapted to different global contexts.

Research examining cybersecurity challenges in developing countries, where older adults may have limited access to technology support and formal cybersecurity resources, could provide important insights for designing low-resource intervention approaches that could benefit older adult populations worldwide.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep709

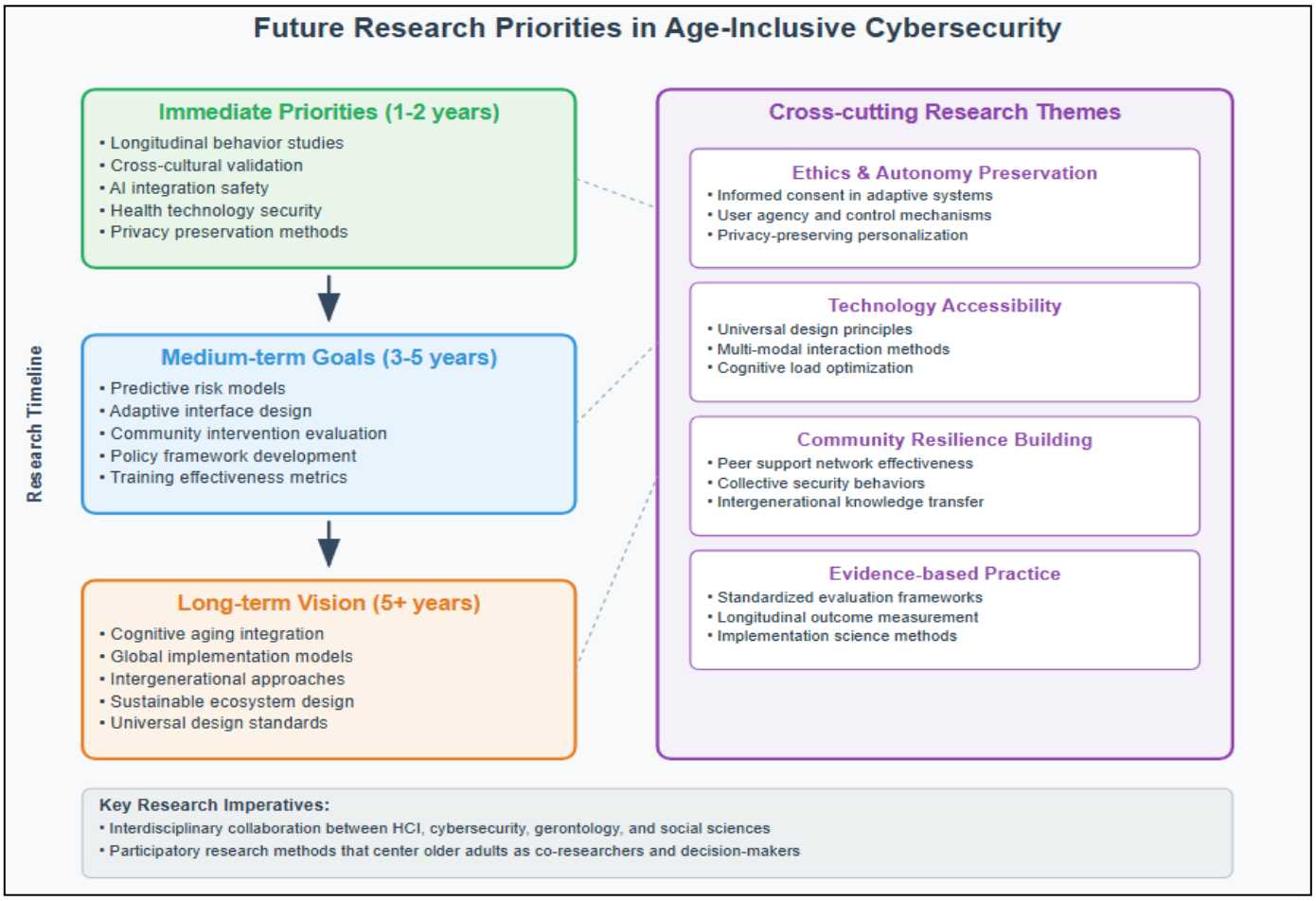

Fig 5 Future Research Priorities in Age-Inclusive Cybersecurity

IV. CONCLUSIONS AND IMPLICATIONS

The challenge of designing age-inclusive cybersecurity represents both an urgent practical need and a significant opportunity for innovation in human-centered security design. This comprehensive review has demonstrated that older adults face unique cybersecurity vulnerabilities that stem from the complex interaction of age-related changes, technology design limitations, and social contextual factors. However, these challenges are not insurmountable obstacles but rather design problems that require innovative, inclusive solutions.

The evidence presented throughout this review consistently points to the inadequacy of traditional cybersecurity approaches for older adult populations. Security systems designed primarily for younger, technically proficient users often create barriers rather than protection for older adults, leading to avoidance behaviors, workaround strategies, and increased vulnerability. The solution lies not in developing separate, simplified systems for older adults, but in embracing universal design principles that create cybersecurity tools that are genuinely usable and effective across the full spectrum of human diversity.

The research reviewed here highlights several key principles that must guide future development of age-inclusive cybersecurity systems. First, recognition of the tremendous diversity within the older adult population is essential. Age-inclusive design cannot assume homogeneity but must accommodate varying levels of technical expertise, cognitive capabilities, physical abilities, and cultural backgrounds. Second, older adults must be recognized as active agents in their own cybersecurity rather than passive recipients of protection. Effective age-inclusive systems must support autonomy and decision-making while providing appropriate guidance and support.

Third, the social dimensions of cybersecurity are particularly important for older adults, who often rely on family, friends, and community networks for technology support. Age-inclusive cybersecurity design must leverage these social resources while avoiding approaches that undermine older adults' independence and confidence. Fourth, the rapidly evolving nature of both cybersecurity threats and technology capabilities requires flexible, adaptive approaches that can evolve with changing needs and circumstances.

The implications of this research extend far beyond the immediate goal of protecting older adults from cybercrime. As populations age globally and digital dependency increases across all age groups, the principles of age-inclusive design become increasingly relevant for creating cybersecurity systems that serve diverse user populations effectively. The research reviewed here suggests that cybersecurity systems

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep709

designed with older adults' needs in mind often provide benefits for users of all ages, supporting the business case for inclusive design approaches.

Furthermore, the challenge of age-inclusive cybersecurity highlights broader questions about technology design, social equity, and digital citizenship. As digital technologies become increasingly central to essential services such as healthcare, banking, and social connection, ensuring that cybersecurity systems are accessible and usable for all population groups becomes a matter of social justice and public policy.

The path forward requires sustained collaboration among researchers, practitioners, policymakers, and older adult users themselves. The research reviewed in this article provides a foundation for evidence-based practice, but significant gaps remain in our understanding of how to most effectively design, implement, and evaluate age-inclusive cybersecurity interventions. Investment in longitudinal research, cross-cultural studies, and innovative design approaches is essential for continuing progress in this critical area.

Perhaps most importantly, the challenge of age-inclusive cybersecurity requires a fundamental shift in how the technology industry and cybersecurity community conceptualize their responsibilities to users. Moving beyond narrow technical definitions of security effectiveness to embrace broader measures of user empowerment, independence, and quality of life represents a necessary evolution in cybersecurity practice. The evidence presented in this review demonstrates that such an evolution is not only ethically necessary but also technically feasible and potentially beneficial for all users.

As we move forward into an increasingly digital future, the design of age-inclusive cybersecurity systems will play a crucial role in determining whether technology serves as a bridge to enhanced independence and connection for older adults or as a barrier that limits their full participation in digital society. The research reviewed here provides both the evidence base and the inspiration needed to ensure that cybersecurity becomes a tool for empowerment rather than exclusion across the full spectrum of human aging.

REFERENCES

[1]. Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. World Congress on Internet Security (WorldCIS-2017), 51-55. https://doi.org/10.1109/WorldCIS.2017.8357168

[2]. Aletras, N., Karyotis, C., Tsagkias, M., Aroyo, L., & Moens, M. F. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. Cognition, Technology & Work, 23(2), 317-336. https://doi.org/10.1007/s10111-021-00683-y

[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, 61(3), 195-206.

[4]. Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2021). Exploring age and gender differences in ICT cybersecurity behaviour. Information & Computer Security, 29(5), 850-865. https://doi.org/10.1108/ICS-07-2020-0125

[5]. Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391-408. https://doi.org/10.1177/0004865814521224

[6]. Carstens, D. S., McCauley-Bell, P., Malone, L. C., & DeMara, R. F. (2004). Evaluation of the human impact of password authentication practices on information security. Informing Science, 7, 67-85.

[7]. Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Rao, H. R. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. Decision Support Systems, 83, 47-56. https://doi.org/10.1016/j.dss.2015.12.007

[8]. Chen, C. C., Shu, D., Ravishankar, H., Li, X., Agarwal, Y., & Cranor, L. F. (2025). Watch my health, not my data: Understanding perceptions, barriers, emotional impact, & coping strategies pertaining to IoT privacy and security in health monitoring for older adults. Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3706598.3714019

[9]. Chhetri, C., & Motti, V. G. (2021). Identifying vulnerabilities in security and privacy of smart home devices. In International Conference on Human-Computer Interaction (pp. 211-231). Springer.

[10]. Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014). SCENE: A structured approach to creating cybersecurity behavioural interventions. Computers & Security, 59, 164-175. https://doi.org/10.1016/j.cose.2016.02.010

[11]. Cross, C. (2017). 'But I've never sent them any personal details apart from my driver's licence number…': Exploring seniors' attitudes towards identity crime. Security Journal, 30(1), 74-88. https://doi.org/10.1057/sj.2015.23

[12]. Ebner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S., Soliman, A., Woodard, D. L., Turner, G. R., Spreng, R. N., & Oliveira, D. (2020). Uncovering susceptibility risk to online deception in aging. The Journals of Gerontology: Series B, 75(3), 522-533. https://doi.org/10.1093/geronb/gbz076

[13]. Fujs, D., Mihelič, A., & Vrhovec, S. L. R. (2025). SmartICST: A smart information and cyber security training approach for older adults. Education and Information Technologies. https://doi.org/10.1007/s10639-025-13564-y

[14]. Grilli, M. D., McVeigh, K. S., Hakim, Z. M., Wank, A. A., Getz, S. J., Levin, B. E., Ebner, N. C., & Wilson, R. C. (2021). Is this phishing? Older age is associated with greater difficulty discriminating between safe and malicious emails. The Journals of Gerontology: Series B, 76(9), 1854-1864. https://doi.org/10.1093/geronb/gbaa228

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep709

[15]. Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of internet hazards. Educational Gerontology, 36(3), 173-192. https://doi.org/10.1080/03601270903183065
[16]. Jeske, D., Briggs, P., & Coventry, L. (2016). Exploring the relationship between impulsivity and decision-making on mobile devices. Personal and Ubiquitous Computing, 20(4), 545-557. https://doi.org/10.1007/s00779-016-0938-4
[17]. Kropczynski, J., Linehan, C., Nir, B., Wisniewski, P., & Carroll, J. M. (2021). Towards building community collective efficacy for managing digital privacy and security within older adult communities. Proceedings of the ACM on Human-Computer Interaction, 4(CSCW3), 1-27. https://doi.org/10.1145/3432954
[18]. Loi, D., Iversen, A., & Røed, J. (2019). Improving cybersecurity awareness: Tweet length matters. Computers & Security, 86, 139-149. https://doi.org/10.1016/j.cose.2019.06.006
[19]. Mentis, H. M., Madjaroff, G., & Massey, A. K. (2019). Upside and downside risk in online security for older adults with mild cognitive impairment. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 1-13. https://doi.org/10.1145/3290605.3300573
[20]. Mihelič, A., Vrhovec, S. L. R., & Fujs, D. (2024). Cybersecurity competence of older adult users of mobile devices. arXiv preprint arXiv:2403.02459.
[21]. Morrison, B. A., Coventry, L., & Briggs, P. (2020). Technological change in the retirement transition and the implications for cybersecurity vulnerability in older adults. Frontiers in Psychology, 11, 623. https://doi.org/10.3389/fpsyg.2020.00623
[22]. Morrison, B. A., Coventry, L., & Briggs, P. (2021). How do older adults feel about engaging with cyber-security? Human Behavior and Emerging Technologies, 3(5), 1033-1049. https://doi.org/10.1002/hbe2.291
[23]. Morrison, B. A., Nicholson, J., Coventry, L., & Briggs, P. (2023). Recognising diversity in older adults' cybersecurity needs. In ACM International Conference on Information Technology for Social Good (GoodIT '23), September 06-08, 2023, Lisbon, Portugal. ACM. https://doi.org/10.1145/3582515.3609565
[24]. Nägle, S., & Schmidt, L. (2012). Computer acceptance of older adults. Work, 41(Suppl 1), 3541-3548. https://doi.org/10.3233/WOR-2012-0633-3541
[25]. Nicholson, J., Coventry, L., & Briggs, P. (2013). Age-related performance issues for PIN and face-based authentication systems. Conference on Human Factors in Computing Systems - Proceedings, 323-332. https://doi.org/10.1145/2470654.2470701
[26]. Nicholson, J., Coventry, L., & Briggs, P. (2019). If it's important it will be a headline: Cybersecurity information seeking in older adults. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 1-11. https://doi.org/10.1145/3290605.3300579
[27]. Ökereafor, K., & Mekovec, R. (2023). Navigating privacy and data safety: The implications of increased online activity among older adults post-COVID-19 induced isolation. Information, 14(6), 346. https://doi.org/10.3390/info14060346
[28]. Pacheco, E. (2024). Older adults' safety and security online: A post-pandemic exploration of attitudes and behaviors. Journal of Digital Media and Interaction, 7(17), 107-126. https://doi.org/10.34624/jdmi.v7i17.37825
[29]. Percy Campbell, J., Yu, L., Duggan, J., Mentis, H. M., & Thapa, N. (2024). User perception of smart home surveillance among adults aged 50 years and older: Scoping review. JMIR mHealth and uHealth, 12, e48526. https://doi.org/10.2196/48526
[30]. Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers & Security, 136, 103585. https://doi.org/10.1016/j.cose.2023.103585
[31]. Ray, H., Wolf, F., Kuber, R., & Aviv, A. J. (2021). Why older adults (don't) use password managers. 30th USENIX Security Symposium (USENIX Security 21), 73-90.
[32]. Roque, N. A., & Boot, W. R. (2018). A new tool for assessing mobile device proficiency in older adults: The mobile device proficiency questionnaire. Journal of Applied Gerontology, 37(2), 131-156. https://doi.org/10.1177/0733464816642582
[33]. Shillair, R., Cotten, S. R., Tsai, H. S., Winstead, V., Yost, E., & Berkowsky, R. W. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. Computers in Human Behavior, 48, 199-207. https://doi.org/10.1016/j.chb.2015.01.062
[34]. Tural, E., Lu, D., & Cole, D. A. (2021). Safely and actively aging in place: Older adults' attitudes and intentions toward smart home technologies. Journal of Applied Gerontology, 40(12), 1650-1659. https://doi.org/10.1177/23337214211017340
[35]. Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. Cyberpsychology, Behavior, and Social Networking, 15(3), 181-183. https://doi.org/10.1089/cyber.2011.0352