Privacy and Data Security in Everyday Online Services for Older Adults

Jonas Ellefsen
Oslo Metropolitan University, Norway
s315731@oslomet.no

Weiqin Chen
Oslo Metropolitan University, Norway
weiche@oslomet.no

ABSTRACT

Older adults are gradually increasing their online activities and usage of online services, including social media applications, online shopping, and online banking. These online services provide many benefits to older adults, but also introduce challenges and risks related to privacy and data security. These challenges must be understood and addressed for older adults to accept and safely use these services. This paper focuses on older adults' understanding of and experience with privacy and data security in their daily use of online services. Using a qualitative approach, we conducted in-depth interviews with 23 older adults. The thematic analysis showed that although the participants are generally active users of online services, they still have challenges in understanding their rights and applying effective strategies to protect their privacy and data. This study contributes to better understanding of older adults' experiences and challenges in different context and calls for better online service design and government support for older adults to use online services.

CCS CONCEPTS

• **Security and privacy**; • **Human and societal aspects of security and privacy**; • **Social aspects of security and privacy**;

KEYWORDS

Older adults, online services, GDPR, password, cookies

ACM Reference Format:
Jonas Ellefsen and Weiqin Chen. 2022. Privacy and Data Security in Everyday Online Services for Older Adults. In *10th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion (DSAI 2022), August 31–September 02, 2022, Lisbon, Portugal.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3563137.3563149

1 INTRODUCTION

Online services are playing an increasingly important role in the daily lives of older adults, particularly during the COVID-19 pandemic, for maintaining social ties, participating in social activities, shopping, managing health and economic affairs, etc. However, researchers have shown that older adults have less knowledge about internet security hazards [1–3], are more vulnerable to attacks [4], and have more concerns about privacy and data security [5, 6] than younger populations, which further increases older adults' anxiety [7] regarding online services, and digital technology in general. Privacy and data security concerns have been found to negatively affect older adults' acceptance of online services [8, 9] and contribute to a generational digital divide. A recent online survey [10] reveals that 34 % of people aged 50 and older cited privacy concerns as a top barrier for adopting new technology and about two in five are not confident that what they do online remains private.

The European Union's General Data Protection Regulation (GDPR) went into effect in May 2018, and most websites now display cookie consent notices [11] which inform users about a site's cookie use and user-tracking practices. How do older adults handle these cookie consent notices? Do older adults understand what it means to consent or opt out? Furthermore, many applications ask users to define a password that contains upper- and lower-case letters, a numeral, and a special character. Although this can help protect users against intruders, it also makes such passwords difficult, if not impossible, to remember, particularly for older adults with decreased cognitive abilities [12].

Although studies have been conducted concerning privacy and data security for older adults in applications such as social media [13–15], smart home solutions [3, 16, 17], and specific technology for authentication, such as graphical passwords [12, 18], most studies focused on older adults' privacy and data security attitudes, perception, and protection behaviors and strategies used a quantitative method [19, 20] and collected survey data. Frik et al. [16] argued that efforts to address privacy and date security concerns and challenges must build on an in-depth understanding of older adults' perceptions and experiences of managing privacy and data security. Qualitative approaches such as in-depth interviews provide such deeper understanding and complement the findings from quantitative studies [19].

In the study presented in this paper we have carried out semi-structured interviews with 23 older adults and adopted a thematic analysis approach to analyze the interview data to understand their perceptions and experience with privacy and data security in their daily use of online services.

2 RELATED RESEARCH

Studies have shown that privacy and data security concerns can hider older adults' adoption of technology [21–24]. Such concerns have been further investigated regarding different types of applications.

Regarding social media application, privacy and data security concerns are found to be negatively associated with the adoption of social media [25]. Lüders and Brandtzæg [25] summarizes the concerns into two forms: sharing private information with commercial providers of social media and losing control over who can access information shared in one's own network of friends and contracts. Gibson et al. [26] and Xie et al. [27] reported that older users are

DSAI 2022, August 31–September 02, 2022, Lisbon, Portugal

ACM ISBN 978-1-4503-9807-7/22/08.
https://doi.org/10.1145/3563137.3563149

more aware of the need for privacy and the ability to control it. Quan-Haase and colleagues [14, 28] conducted in-depth interviews with 40 older adults in East York, Toronto, Canada, to understand to what extent privacy concerns could be a barrier to social media adoption. They found that social media users and non-users shared similar privacy concerns, including unauthorized access to personal information and information misuse. Their participants were mostly concerned about security privacy concerns followed by institutional privacy concerns and only minimally concerned about social privacy. Protection strategies older adults used include avoiding social media (non-users) and limiting the information they shared (users).

Regarding online banking services, Knowles and Hanson [29] found that older adults were resistant to online banking due to mistrust which was partly due to security concerns (e.g., hacking) and partly due to a lack of confidence in one's ability as a user. These findings were confirmed in a study that identifies factors that influence each generation's acceptance and use of online banking [30] where trust was found to matter more to older adults than younger generations in determining their intentions to use online banking. In a study compared the perception of risks across generations [30], older adult populations were more suspicious of online security, highly aware of threats such as spam, e-mail scams and etc. and less confident in their abilities to effectively protect themselves.

3 METHODS

We adopted a qualitative approach using semi-structured interviews to collect data on the experiences of older adults in managing privacy and data security when using online services. Before we recruited participants, we submitted study-related documents, including the interview guide, information sheet, consent form, and data management methods and plan (e.g. how and where data are stored and processed, who has access to the data, and how long are the data stored) to the national ethical committee. The national ethical committee examined the study according to GDPR and national ethical requirements concerning scientific data privacy and security. After the study was approved, we distributed an invitation to participate via an organization for older adults with members all over the country. The invitation included information sheet and contact persons for the project. Interested members contacted the researchers, and we answered questions about the study via email or telephone call.

Twenty-three volunteers (P1-P23) were recruited for this study using a convenience sampling method. We conducted interviews during February and early March 2021 with a semi-structured format focusing on collecting data about participants' awareness, experience, knowledge, concerns, and strategies in relation to privacy and data security when using online services. We were particularly interested in their everyday privacy and data security management, such as password and cookies when using social media, visiting websites, doing online shopping, and using online banking services.

Each interview lasted from 26 to 88 minutes. We collected a total of 17 hours of audio interview data. Written field notes were also taken during and after each interview. The audio data were used to assist researchers to fill in blank spaces in the field notes and clarify the intended meaning from the original source in case of ambiguity and inconsistencies. The thematic analysis was conducted by two researchers, and any disagreements concerning coding and themes were resolved by discussion. At the analysis stage, we also contacted some of the participants to clarify some answers they provided during the interviews.

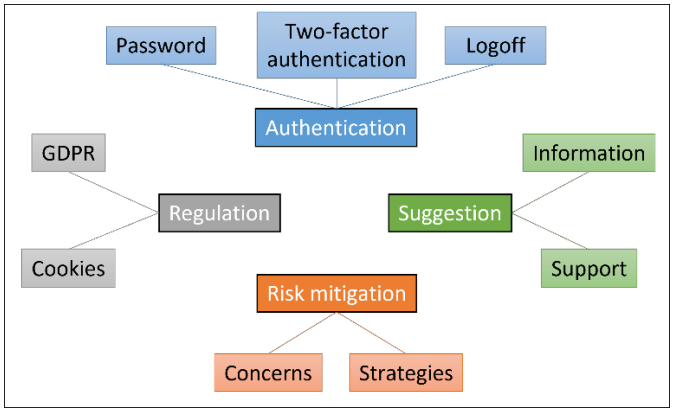

Figure 1: Final themes

4 RESULTS

4.1 Participants

The 23 participants included 14 males and 9 females. Their age range was 69–83 years (mean = 75). The participants had at least 15 years of internet use experience. All except one participant use social media applications, including Facebook, Instagram, Twitter, WhatsApp, and LinkedIn; 20 reported that they use Facebook, and 15 considered themselves passive users of social media (i.e., they only watch and do not post). Seventeen participants read online newspapers and do online shopping; six do not shop online. All participants use online banking services. They also reported using mobile devices, including smart phones, tablets, and laptop and desktop computers.

4.2 Themes

The analysis presented in this paper focuses on what older adults know in relation to privacy and data security when using online services, with particular emphasis on their everyday experiences. Four main themes emerged from the thematic analysis: Authentication, Regulation, Risk mitigation, and Suggestion (Figure 1). The first main theme Authentication has three subthemes: Password, Two-factor authentication, and Logoff. The second main theme Regulation has two subthemes: GDPR and cookies. The third main theme Risk mitigation has two subthemes: Concerns and Strategies. The fourth main theme Suggestion has two subthemes: Information and Support.

4.2.1 *Authentication.*

Password. Passwords were found to be challenging for all participants. The main challenges included remembering passwords (12 participants), creating unique passwords (5 participants), and changing passwords (5 participants). One participant directly linked passwords to identify theft. When asked how they remembered

Table 1: Numbers of participants who actively logged out of their accounts after use

Frequency	Social media account	Online banking account
Always	2	11
Often	1	9
Sometimes	3	1
Never	14	0
Did not specify	3	2

passwords, 15 reported that they wrote their passwords down somewhere although they were aware of the risks. One preferred to use biometric authentication methods such as a fingerprint. Five participants reported that they used a password manager, such as LastPass and Norton Password Manager. Two participants reported using the built-in password managers in the Chrome and Firefox web browsers. Eight participants did not use a password manager, but four of them were interested in using one. Three had tried password managers but found them too complicated to learn and use. Only two reported that because they could remember their passwords they neither wrote them down nor used a password manager. Participants reported difficulties in coming up with unique passwords that fulfill the password composition requirements which also made the passwords more difficult to remember.

> *Finding good, secure passwords is hard.* (P22)
>
> *You need to have multiple passwords, and they need to be different all the time.* (P10)

Participants also found the experience of changing passwords cumbersome and frustrating. They had to create a new unique password, which was already a challenge. When they had managed to create new passwords, they also had to remember to update where they had written down their previous passwords. P2 reported that he had forgotten where he wrote down his passwords.

Two-factor authentication. All participants used two-factor authentication, although they found it tedious in the beginning and could cause a "*delay*" in the log-in process because it added an extra step. Nevertheless, they felt safer and more reassured and saw more pros than cons. They used the authentication method for different purposes such as online shopping, mobile applications, and online banking.

Logoff. When participants were asked whether they actively logged off from their accounts after use, their responses showed that they handled their social media accounts and their online banking accounts differently (Table 1). Participants stated that they did not care about social media accounts, but they considered their personal finances (e.g., banking) and health information especially important to protect.

4.2.2 Regulation.

GDPR. Eleven participants reported that they had heard about the GDPR and knew what it meant, but did not know the details. Only one could explain the GDPR, because s/he had learned about it at work. Another participant reported that s/he knew her/his right concerning online data and had used an information removal service to remove her/his online data.

Cookies. 11 responded that they accepted all cookies. The participants reported different reasons for accepting cookies when visiting websites. Some felt that they had to accept them, the cookie information provided by websites was too difficult to read, or changing preferences took too much time. For example,

> *I feel like I have to accept in order to proceed.* (P4)
>
> *I accept everything. The information is hard to read.* (P11)

Others accepted cookies simply because they did not understand them.

> *I do not know much about it, so I accept.* (P3)

Seven participants reported that they mainly accepted cookies but sometimes changed preferences. They accepted cookies on familiar websites and websites they trusted and changed their preferences for unfamiliar ones. Some also accepted cookies when they were in a hurry. For example,

> *I accept cookies on familiar websites, otherwise change preference.* (P1)
>
> *I tend to change preference. If I don't have time, I accept.* (P20)

However, the participants also found that checking and changing preferences were complicated (P17) and time-consuming (P20, P21 and P22). The other five participants responded that they mainly rejected cookies or changed preferences.

> *I tend to turn off most data they want to collect, and later turn them on in options as I see fit. . . . I do not want third parties to have my information.* (P1)

P13 also reported that he consistently changed his preferences for all websites and understood full access and limited access.

4.2.3 Risk Mitigation.

Concerns. Out of the 23 participants, 10 responded that they felt safe online, but were aware of the possible risks, such as leaking of personal information, phishing, online surveillance, identity theft, and online fraud. Only one reported that s/he had no concerns because s/he does *not have anything to hide* (P10). Others were more worried about the risks and did not feel completely comfortable using online services.

> *I do not feel safe. Too much online fraud, and I have to register everywhere.* (P9)

Strategies. The participants also reported using various protection strategies. Being generally cautious when interacting with online services was one of the basic strategies, including being selective about where to shop online, using familiar and trusted

websites, not sharing personal, financial, and health information, and checking before clicking on links. In addition, strategies such as checking and changing privacy settings (8 participants), checking HTTP or HTTPS in the URL (4 participants), and using protective tools and online resources such as an URL scanner and information from consumer and data protection authorities (12 participants) were identified from the interview data.

4.2.4 *Suggestion.*

Information. Participants reflected on their knowledge and expressed wishes and suggestions for learning and better protecting their privacy and data security. They highlighted information and instructions from the government and authorities for older adults. For example,

> *The authorities, as well as organizations, should give more attention towards passwords and access control, especially for seniors. . . We need aids, like instructional videos. I would like if the authorities gave us some tips on what applications we should use regularly, to help us with technology and cybersecurity.* (P2)

Support. Participants also commented that online services should provide better support for privacy and data security protection. For example,

> *When you sign up for something like Facebook, you should be guided through their settings to set your preferences. . . This would help so there is as little information as possible about the individual, to protect their privacy and identity.* (P22)

5 DISCUSSION

Compared with previous studies such as [14, 28] which focused on privacy and data security in social media applications, our study showed that older adults act differently when they use social media and when they use what they consider privacy- and security-critical online services, such as online banking and health applications. This was demonstrated by the high number of participants who actively log out of their accounts in online banking services comparing with those who do not log out of their accounts in social media applications.

Frik et al. [16] found that older adults often experience usability issues or technical uncertainties when mitigating security and privacy risks. Participants in our study also reported such issues, including password managers being very complicated to set up and use. These challenges have also been identified in the study investigating older adults' motivation in using (or not using) password managers [31]. Concerning authentication methods, only one participant in our study reported that s/he prefer biometric methods, which is different from [32] where 61.11% of older adults reported that they preferred biometric options. Very few studies have focused on the use (or not use) biometric authentication methods by older adults, which calls for further research on this topic.

Our study also showed that participants found understanding, checking, and changing privacy and data protection preferences in cookies complicated and time-consuming. Without a good understanding of the cookies, they are not able to give informed consent. Neumann and Davies [33] in their policy brief recommended that the GDPR should be reviewed in detail to determine what extensions are needed to meet the requirements of older adults and guidelines should be established to help developers that are tackling data protection issues of older adults.

The participants in our study further expressed their wishes for better information and training from authorities and online service providers [14, 28]. Such support can help increase self-efficacy that empowers older adults to make informed decisions. In terms of protection strategies, findings indicate that the participants use more active strategies than those identified by Frik et al. [16]. This is demonstrated by the number of participants who check change privacy settings and those who check HTTP or HTTPS in the URL in order to protect privacy and data security.

This study has several limitations. In addition to the convenience sampling and the small number of participants, we recruited participants only from one national organization for older adults. The organization offers training courses to its members. Therefore, the participants may be better equipped with knowledge and skills than older population in general in managing privacy and data security. This was demonstrated by the high number of participants who use online banking, password manager, and who were aware of the GDPR. However, there are still many older adults who have low digital literacy. For example, according to 2020 statistics, 2.84 million people age 65 and older in the United Kingdom (UK) have never used the internet [34]. Future research, therefore, should recruit more participants with different levels of experience and knowledge to reflect the diversity of the older population.

6 CONCLUSION AND FUTURE WORK

This paper presents a study on older adults' experience with privacy and data security in their everyday online activities. The results show that although our participants are in general active users of online services such as social media and online banking, they still have challenges in creating and remembering passwords, understanding and managing cookies and using effective strategies to protect their privacy and data security when using online services. They hope for better information and training from authorities and better designed services and easy to understand cookie information in order to make better informed decisions. There are many factors that affect older adults' awareness and knowledge in privacy and data security, as demonstrated in previous studies [19, 20]. Future research should investigate the impact of these factors by combining qualitative and quantitative approaches and collecting data from a more representative sample of older population. The findings in this study also indicate that adequate training and suitable technology design that address the needs and preferences of this user group are important for their acceptance and adoption of digital technology, as pointed out in previous studies [14, 16]. The study contributes to a better understanding of older adults' experience, concerns, and needs in terms of privacy and data security in their everyday use of digital services.

The overall objective of the study is to increase older adults' awareness and knowledge of how to protect their security and privacy in their digital everyday life, provide input to the online services so that their designs include the necessary and adequate

support for this user group, and inform policy and strategies concerning training programs for the older population.

ACKNOWLEDGMENTS

The authors would like to thank Seniornett Norway for helping recruit participants. Special thanks to all the participants who shared their valuable experiences and suggestions with us. The authors would also like to thank the anonymous reviewers for their insightful and constructive feedback.

REFERENCES

[1] Grimes, G. A., Hough, M. G., Mazur, E. and Signorella, M. L. Older adults' knowledge of internet hazards. Educational Gerontology, 36, 3 (2010), 173–192.
[2] Garg, V., Lorenzen-Huber, L., Camp, L. J. and Connelly, K. Risk communication design for older adults. Gerontechnology, 11, 2 (2012), 166–173.
[3] Lorenzen-Huber, L., Boutain, M., Camp, L. J., Shankar, K. and Connelly, K. H. Privacy, technology, and aging: A proposed framework. Ageing International, 36, 2 (2011), 232–252.
[4] Grimes, G. A., Hough, M. G. and Signorella, M. L. Email end users and spam: Relations of gender and age group to attitudes and actions. Computers in Human Behavior, 23, 1 (2007), 318–332.
[5] Hoofnagle, C., King, J., Li, S. and Turow, J. How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? SSRN (2010).
[6] Walters, N. Maintaining privacy and security while connected to the Internet. City, 2017.
[7] Chou, W. H., Lai, Y. T. and Liu, K. H. Decent digital social media for senior life: A practical design approach. City, 2010.
[8] Chen, K. and Chan, A. H. S. Use or non-use of gerontechnology-A qualitative study. International Journal of Environmental Research and Public Health, 10, 10 (2013), 4645–4666.
[9] Nef, T., Ganea, R. L., Müri, R. M. and Mosimann, U. P. Social networking sites and older users - A systematic review. International Psychogeriatrics, 25, 7 (2013), 1041–1053.
[10] Kakulla, B. Tech Trends and the 50-plus. AARP Research, 2021.
[11] Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F. and Holz, T. We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. City, 2019.
[12] Renaud, K. and Ramsay, J. Now what was that password again? A more flexible way of identifying and authenticating our seniors. Behaviour & Information Technology, 26, 4 (2007), 309-322.
[13] Chakraborty, R., Vishik, C. and Rao, H. R. Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. Decision Support Systems, 55, 4 (2013), 948–956.
[14] Quan-Haase, A. and Elueze, I. Revisiting the Privacy Paradox: Concerns and Protection Strategies in the Social Media Experiences of Older Adults. Association for Computing Machinery, City, 2018.
[15] Van den Broeck, E., Poels, K. and Walrave, M. Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. Social Media + Society, 1, 2 (2015), 1-11.
[16] Frik, A., Nurgalieva, L., Bernd, J., Lee, J. S., Schaub, F. and Egelman, S. Privacy and Security Threat Models and Mitigation Strategies of Older Adults. USENIX Assoc., City, 2019.
[17] McNeill, A., Briggs, P., Pywell, J. and Coventry, L. Functional privacy concerns of older adults about pervasive health-monitoring systems. In Proceedings of the Proceedings of the 10th International Conference on PErvasive Technologies Related to Assistive Environments (2017). ACM, [insert City of Publication],[insert 2017 of Publication].
[18] Carter, N. J. Graphical Passwords for Older Computer Users. In Proceedings of the Adjunct Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology (UIST '15 Adjunct) (2015). ACM, [insert City of Publication],[insert 2015 of Publication].
[19] Huang, H. Y. and Bashir, M. Surfing Safely: Examining Older Adults' Online Privacy Protection Behaviors. Proceedings of the Association for Information Science and Technology, 55, 1 (2018), 188– 197.
[20] Zeissig, E. M., Lidynia, C., Vervier, L., Gadeib, A. and Ziefle, M. Online Privacy Perceptions of Older Adults. Springer, City, 2017.
[21] Cantor, M. No information about me without me: technology, privacy, and home monitoring. Generations, 30, 2 (2006), 49–53.
[22] Chung, J. E., Park, N. and Wang, H. Age differences in perceptions of online community participation among non-users: an extension of the technology acceptance model. Computers in Human Behavior, 26, 6 (2010), 1674–1684.
[23] Niehaves, B. and Plattfaut, R. Internet adoption by the elderly: Employing IS technology acceptance theories for understanding the age-related digital divide. European Journal of Information Systems, 23, 6 (2013), 708–726.
[24] Chen, H.-T. and Chen, W. Couldn't or wouldn't? the influence of privacy concerns and self-efficacy in privacy management on privacy protection. Cyberpsychology, Behavior, and Social Networking, 18 (2015), 13-19.
[25] Lüders, M. and Brandtzæg, P. B. "My children tell me it's so simple": a mixed-methods approach to understand older non-users' perceptions of social networking sites. New Media & Society (2014).
[26] Gibson, L., Moncur, W. and Forbes, P. Designing Social Networking Sites for older adults. In Proceedings of the The 24th BCS Interaction Specialist Group conference (Dundee, 6–10 September, 2010), [insert City of Publication],[insert 2010 of Publication].
[27] Xie, B., Watkins, I. and Golbeck, J. Understanding and changing older adults' perceptions and learning of social media. Educational Gerontology, 38, 4 (2012), 282–296.
[28] Quan-Haase, A. and Ho, D. Online privacy concerns and privacy protection strategies among older adults in East York, Canada. Journal of the Association for Information Science and Technology, 71, 9 (2020), 1089-1102.
[29] Knowles, B. and Hanson, V. L. Older Adults' Deployment of 'Distrust'. ACM Trans. Comput.-Hum. Interact., 25, 4 (2018), Article 21.
[30] Jiang, M., Rifon, N. J., Cotten, S. R., Alhabash, S., Tsai, H.-Y. S., Shillair, R. and LaRose, R. Bringing older consumers onboard to online banking: a generational cohort comparison. Educational Gerontology, 48, 3 (2022), 114-131.
[31] Ray, H., Wolf, F., Kuber, R. and Aviv, A. J. Why older adults (don't) use password managers. ArXiv (2021).
[32] Ahmed, E., DeLuca, B., Hirowski, E., Magee, C., Tang, I. and Coppola, J. F. Biometrics: Password replacement for elderly? In Proceedings of the IEEE Long Island Systems, Applications and Technology Conference (LISAT) (2017), [insert City of Publication],[insert 2017 of Publication].
[33] Neumann, V. and Davies, N. A. J. Policy Brief: Privacy implications of technologies to address social isolation amongst older adults (2018).
[34] Prescott, C. Internet users, UK: 2020. Retrieved from https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2020.