ACIT5900

MASTER THESIS

in

Applied Computer and Information Technology

(ACIT)

May 2021

Universal Design of ICT

Privacy and Data Security in Everyday Online Services for Older Adults

Jonas Ellefsen

Department of Computer Science

Faculty of Technology, Art and Design

Preface

When I started my journey at OsloMet, what was then called Oslo and Akershus University College, I had little idea of what it was going to be like. The first years of my bachelor's, I was thinking of "just getting through it" to finish my degree and then find a job. One thing I knew for certain was to never apply for a master's degree. Yet here I am writing the preface to my master thesis. During my bachelor's I started getting a predilection for human-centered and universal design, which eventually led me to apply for the *Universal Design of ICT master program*. By the time I was going to write my master thesis, I had gotten increasingly interested in security, and had started looking more into privacy regulations and security protocols. Luckily, I was able to find a topic for my master thesis which included my core specialization in universal design AND data security. While writing my master thesis I got to meet a lot of interesting people, and I would love to thank all of them.

I was fortunate to get in touch with Seniornett, where I got introduced to Siri Kessel. Siri helped me in structuring the interviews, giving feedback and conveying information from me to Seniornett. I was really surprised by the lovely members of Seniornett who reached out to me and wanted to contribute to this research. It was a pleasure listening to your stories and getting to know you all. Thank you very, very much.

Lastly, I want to thank my supervisor, Weiqin Chen. During this semester I have learned so much from our weekly meetings on Zoom about preparing for and conducting interviews, academic writing, and you have taught me that research can be a lot of fun. I also had the pleasure of writing a paper with you, and I am grateful to be a part of it.

Jonas Ellefsen

Jonas Ellefsen - Oslo, 14.05.2021.

Abstract

Older adults (people aged 65+) are using a wider range of digital technologies and online services than before. After the COVID-19 outbreak and the social distancing measures, online services have become increasingly important. Online services enable participation in digital social events, maintenance of social connections, and management of health and financial affairs. The goal of this research is to understand the experiences of older people regarding privacy, authentication and risk management in everyday online services. In achieving this, a qualitative method was used, and 23 semi-structured interviews were conducted. The research discovered that our older participants are more active on social media platforms, use a wider range of authentication methods, and have more knowledge on protecting their privacy than what related literature indicates. Moreover, surveillance, fraud, and identity theft were some of the main concerns they encountered. The results indicate that instructions, adequate training and well-designed technical solutions is important in understanding and mitigating risks, which further contribute to the acceptance and adoption of digital technologies for older adults. This research suggests that good perception of privacy, authentication and risk management is achieved by including older adults in the process of designing new technology and arranging training courses to help older adults in managing digital technologies.

Table of Contents

List of figures

List of tables

1 Introduction

Today, we are experiencing a global aging phenomenon. The older population is rapidly increasing all over the world (United Nations, 2020), and the life expectancy of most people globally have increased way beyond their sixties (WHO, 2018). People are often considered *old* when aged 65 years old or older (Encyclopaedia Britannica, n.d.). However, it changes depending on where one is in the world. In Norway, adults are defined as old when reaching the *retirement age* of 67 years old. *Older adults* are often identified as the people between the age of 67-79 years old, and the people aged 80 years or older is considered *elderly* (Statistics Norway, 1999). In Thai society, however, the elderly is known as those aged 60 years or older (Ministry of Social Development and Human Security, 2003). According to the United Nations (2020), 703 million people were aged 65 or older in 2019, and the group of people aged 80 or older will be growing much faster than in previous years. By 2050, the world's population over 60 years is expected to be doubled of what it was in 2015 (WHO, 2018).

The coronavirus disease (COVID-19) came to light in December 2019 and was identified in January 2020 (Norwegian Institute of Public Health, 2021; WHO, n.d.). COVID-19 has changed the daily life and activities of older adults, as it has required them to stay more at home, having less physical contact with family and friends, and restricting other social activities (Brooke & Jackson, 2020). Because of this, online services are playing an increasingly important role in the daily lives of older adults. Online services enable participation in digital social events, maintenance of social connections, management of health and financial affairs. However, as everyday lives are more affected by online services, a higher level of technology skills is required. This creates a digital gap between the younger generation and the older adults. Seeing as the seniors did not grow up using the digital technologies utilized today, many often feel excluded and choose to opt out of using new technologies entirely (Seifert, 2020). Furthermore, older adults have less knowledge about internet security risks, are more vulnerable to online assaults, and have more concerns regarding their privacy and data security than the younger generation (Grimes, Hough, Mazur, & Signorella, 2010; Walters, 2017).

This study connects universal design and accessible technology, and data security and online privacy. In human-computer-interaction (HCI), universal design reflects on the idea of a conscious effort to design products which address the challenges faced by users with disabilities, and the special requirements of an ageing population (Stephanidis & Akoumianakis, 2001). Everybody should be able to use digital technologies and online services. As people are more reliant on portable devices, the importance of well-designed authentication methods is increasing. However, several of the authentication methods used today present accessibility barriers for people with disabilities (Andrew, Watson, Oh, & Tigwell, 2020). Security should be an enabler for digital technologies, instead of introducing barriers. The goal of this research is to understand the experiences of older people regarding privacy, authentication and risk management in everyday online services.

In this thesis, the relevant literature of the study will be presented, followed by the methodologies used to conduct the study. Further, a result section will present all the important findings. In the discussion, a reflection is made on findings identified in the literature review, which is compared to this study's findings, and future work is introduced. Lastly, the conclusion is presented, which will answer to the research goal of the thesis.

2 Background

In this section, a thorough description of the background information is given.

2.1 General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a legislation made by the European Union (EU). The legislation was put into effect on May 25th, 2018. GDPR contains documentation which regulates how personal data and human consent must be handled. In addition, it refers to the interaction between the human and the computer system (Sanchez-Rola, et al., 2019; Soe, Nordberg, Guribye, & Slavkovik, 2020). In short terms, the main takeaways from the GDPR data protection principles include fairness, lawfulness and transparency. The GDPR advocates for organizations to ensure data protection “by design and by default” (Politou, Alepis, & Patsakis, 2018).

Similar to what the EU did by legislating the GDPR, the United States (US) wanted to secure the privacy of their consumers. By doing so, the California Consumer Privacy Act (CCPA) was introduced the same year as the GDPR came to effect (2018). However, it did not come become effective until January 1st, 2020. The privacy regulations included the right to know, delete and opt-out of personal information. Furthermore, the regulation advocated for the right to non-discrimination among its consumers (Department of Justice, n.d.).

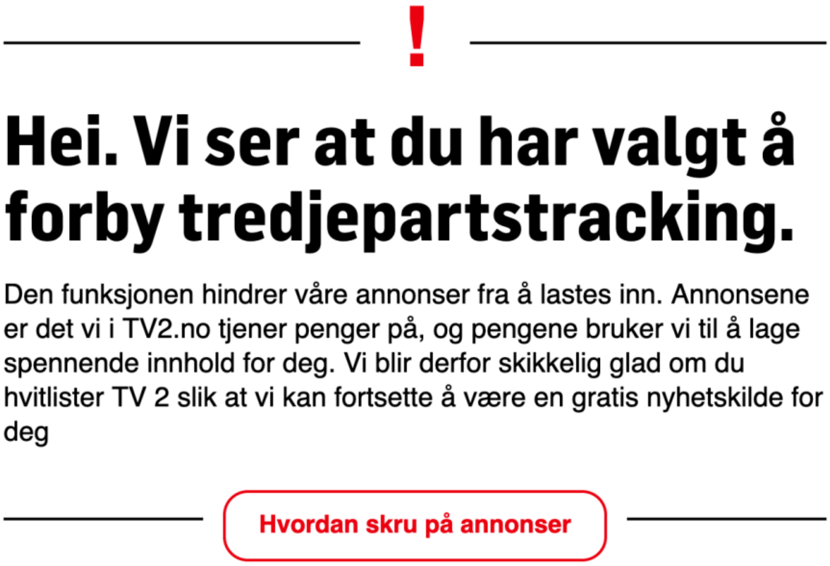
In response to the GDPR legislation and CCPA regulation, consumers were often updated on organizations’ changes to processing of data, and websites started to display cookie consent notices which needed to be managed by the users (Soe, et al., 2020). In the next sub-section, a more comprehensive explanation of cookies and its consent notices is given.

2.1.1 Cookies

HTTP (Sanchez-Rola, et al., 2019), session or web cookies, were invented in 1994 to further enable the development and maintainability of websites and have been a key part in the evolution of web applications. Today, the main goal and purpose of cookies is to deliver targeted ads to the web user (Cahn, Alfeld, Barford, & Muthukrishnan, 2016).

There are two types of cookies which are commonly used in web applications, first-party and third-party cookies. First-party cookies are those placed by the domain; a common example of which is used to enable the shopping cart found in e-commerce websites (Cahn, et al., 2016). The third-party cookies are placed on the first-party’s websites but are only used and analyzed by the third-party organization. Third-parties tend to see a bigger picture of the users' browsing habits, as they have access to the browser history wherever the third-party cookie is placed. A common example of this is websites that use Google Analytics, where a cookie is placed by Google to analyze user behavior (Hu & Sastry, 2019).

Although cookies can be beneficial in improving services and products (Sipior, Ward, & Mendoza, 2011), they limit the user's online privacy. In addition, cookies may be perceived as disturbing and annoying to some users. Researchers have found "dark patterns" when analyzing webpages and cookies, as the cookie notices often obstruct or interfere with the user interface and user experience (Sanchez-Rola, et al., 2019; Soe, et al., 2020). The first example of which, is cookie consent notices which are perceived as *nagging* (see Figure 2.1). In cases where the user denies their consent, the parties are actively trying to change the user's mind.

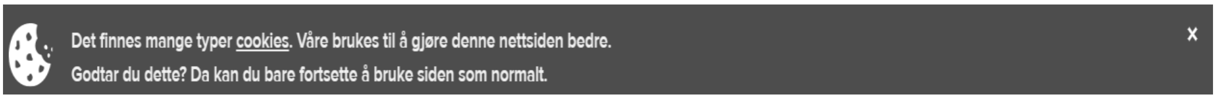


Hei. Vi ser at du har valgt å forby tredjepartstracking.

Den funksjonen hindrer våre annonser fra å lastes inn. Annonsene er det vi i TV2.no tjener penger på, og pengene bruker vi til å lage spennende innhold for deg. Vi blir derfor skikkelig glad om du hvitlister TV 2 slik at vi kan fortsette å være en gratis nyhetskilde for deg

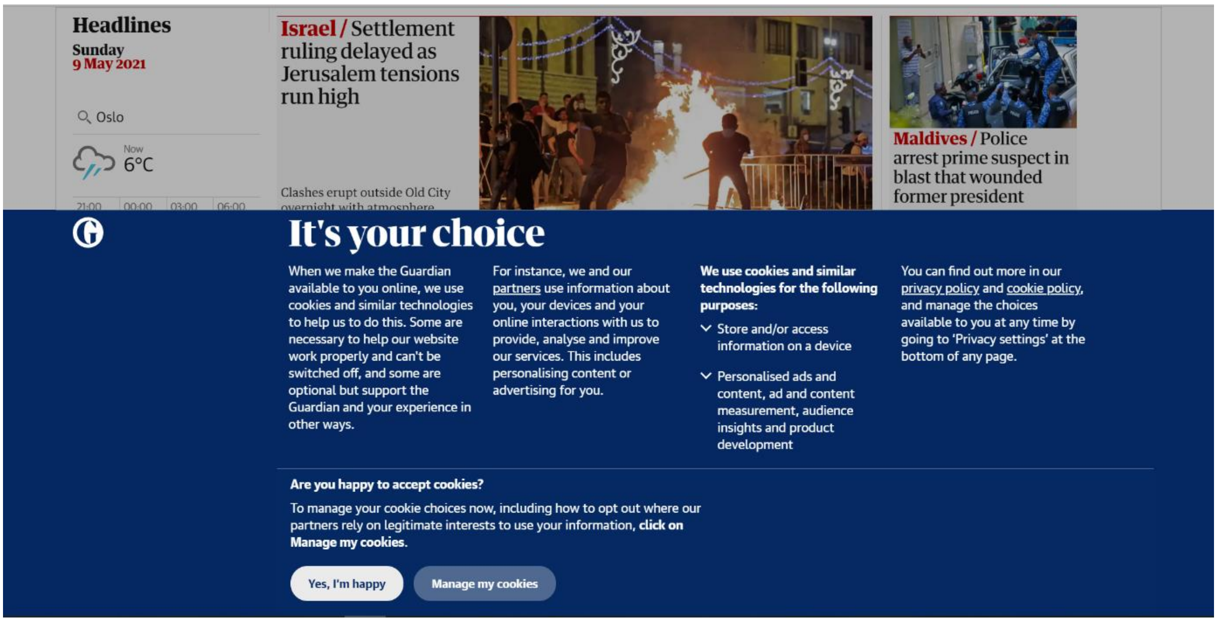
Figure 2.1 Screenshot. An example of a nagging cookie notice. The text reads "Hi. We see you have chosen to reject third-party tracking." Retrieved from Soe, et al. (2020).

The next example is the *sneaking* cookie consent notice. The notice often reads "by using our website, you accept our policies", which disables the user in changing their cookie preference (see Figure 2.2). Lastly, the final example is the *forced action* cookie consent notice. As the name suggests, the user needs to perform a certain action to proceed. Looking at Figure 2.3, most of the view is hindered by the cookie notice, the user can however choose to accept or change their cookie consent preference (Soe, et al., 2020).



Det finnes mange typer cookies. Våre brukes til å gjøre denne nettsiden bedre.
Godtar du dette? Da kan du bare fortsette å bruke siden som normalt.

Figure 2.2 Screenshot. An example of a sneaking cookie notice. The text reads "There are many types of cookies. Ours are used to make this website better. Do you accept? Then you can continue to use the site as usual." Retrieved from https://www.sio.no/.



Israel / Settlement ruling delayed as Jerusalem tensions run high

Clashes erupt outside Old City overnight with atmosphere

Maldives / Police arrest prime suspect in blast that wounded former president

It's your choice

When we make the Guardian available to you online, we use cookies and similar technologies to help us to do this. Some are necessary to help our website work properly and can't be switched off, and some are optional but support the Guardian and your experience in other ways.

For instance, we and our partners use information about you, your devices and your online interactions with us to provide, analyse and improve our services. This includes personalising content or advertising for you.

We use cookies and similar technologies for the following purposes:

- Store and/or access information on a device
- Personalised ads and content, ad and content measurement, audience insights and product development

You can find out more in our privacy policy and cookie policy, and manage the choices available to you at any time by going to 'Privacy settings' at the bottom of any page.

Are you happy to accept cookies?

To manage your cookie choices now, including how to opt out where our partners rely on legitimate interests to use your information, **click on Manage my cookies**.

Figure 2.3 Screenshot. An example of a forced action cookie consent notice. Retrieved from https://www.theguardian.com/.

2.2 Authentication

Authentication is the process verifying the user's identity (ID). Three factors of user authentication are often identified as: something the user knows (password), something the user has (e.g., smart card), or something the user is (biometric). When a user is trying to get access to a system, they need to provide the registered ID (often e-mail or an ID-number) and the given authentication method. If it matches what is registered in the system they are trying to access, they are authenticated (Lal, Prasad, & Farik, 2016). Each authentication method will be explained more in-depth in separate sub-sections, starting with passwords.

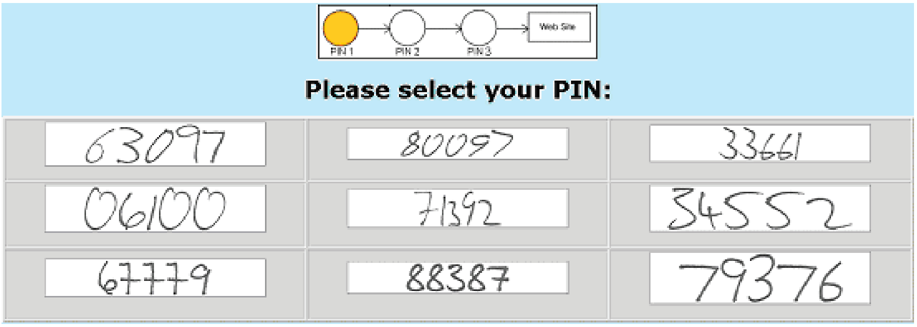
2.2.1 Passwords

Text and number-based passwords is the most widely used method of authentication in computer systems (Carter, et al., 2017; Komanduri, et al., 2011). As with all authentication methods, passwords' purpose is to deny unauthorized parties into the computer system. To limit the possibility of adversaries getting access to the users' password, the passwords need to be secure. In achieving this, password policies must be followed (Marky, Mayer, Gerber, & Zimmermann, 2018). The most common requirements in password policies include a minimum number of characters, the use of particular character classes (e.g., lower- and uppercase letters, numbers and symbols), and the password combination cannot be found in a list of regularly used passwords (Shay, et al., 2016). A list of the 20 most commonly used passwords in the year of 2020 is displayed in Table 2.1. However, password policies are often too inflexible, making passwords hard to create and hard to remember for the users of the computer system. In addition, people, especially older adults, struggle to match their passwords and accounts. This often results in them reusing the same password for multiple services. The policies should be redesigned to enable the users in creating reliable and strong passwords, using principles from HCI (Inglesant & Sasse, 2010; Topkara, Atallah, & Topkara, 2007).

Table 2.1 The 20 most common passwords in 2020. Retrieved from https://nordpass.com/most-common-passwords-list/.

1	123456	**2**	123456789	**3**	picture1	**4**	password
5	12345678	**6**	111111	**7**	123123	**8**	12345
9	1234567890	**10**	senha	**11**	1234567	**12**	qwerty
13	abc123	**14**	Million2	**15**	000000	**16**	1234
17	iloveyou	**18**	aaron431	**19**	password1	**20**	qqww1122

Unlike the common text-based passwords, visual and graphical passwords use images and graphics for authentication. The development of these methods came from the idea that pictures are more secure than words (Renaud & Angeli, 2009). Studies have found that visual and graphical passwords have better usability than other common passwords, and they are more secure than 4-digit PINs and short text passwords (Carter, et al., 2017; Chiasson, et al., 2009). An example of how a visual password can be used is shown in Figure 2.4. In this example, the user has written down a PIN in advance and need to recognize their handwriting among all the options in order to authenticate. This process is iterated 3 times before entering the website.



Please select your PIN:

63097	80097	33661
06100	71392	34552
67779	88387	79376

Figure 2.4 An example of a visual password. The user is prompted with 9 PINs and needs to select the correct option. Retrieved from Renaud & Angeli (2009).

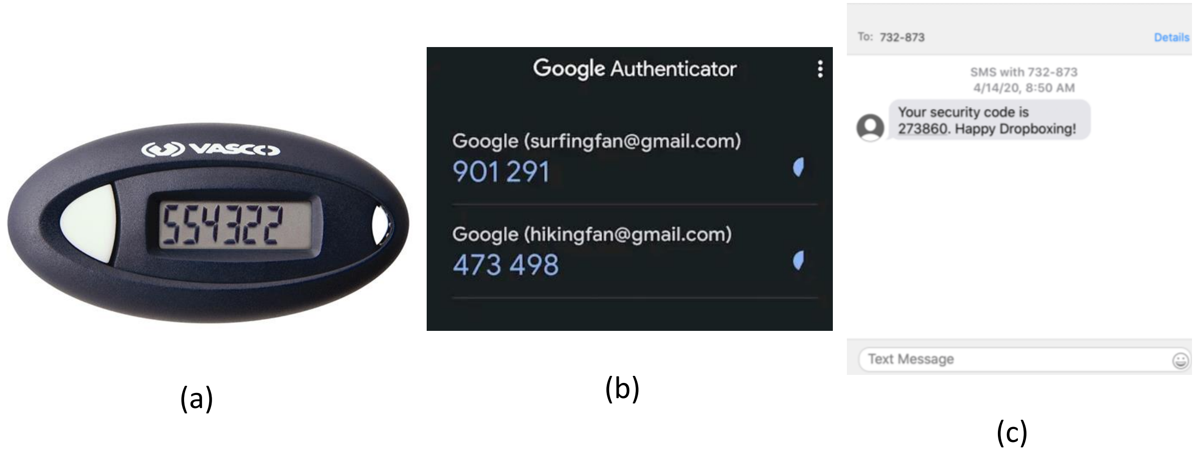
Many users struggle with passwords and cope for strategies such as reusage or even writing the passwords down. By writing down passwords, it allows the user to select a more complex password than what they otherwise would try to remember. Although this strategy makes passwords more secure, it also introduces another risk. If an unauthorized party discovered the list of passwords, they would no longer be confidential. However, there are other ways of managing one's passwords - an example of this is using a password manager. This tool enables the user to store already existing password in a more secure way and generate new ones (Stobert & Biddle, 2018). In order to access the password manager, the user needs a master username and password. Further, the manager maintains a database of all the user credentials (IDs or usernames), what application it relates to, and the secure password. To ensure a secure password management system, a decryption/encryption method is used, meaning the credentials are not stored in clear text (Li, He, Akhawe, & Song, 2014).

2.2.2 Biometrics

Biometric authentication is a security process where the user is identified based on their characteristic physiological or behavioral parameters (Bhattacharyya, Ranjan, Alisherov, & Minkyu, 2009). Physiological biometrics include fingerprints, face recognition and iris-scan; behavioral biometrics include voice recognition and signature recognition. Among the different biometric authentication methods, fingerprint is the most widely used (Lal, Prasad, & Farik, 2016). Moreover, biometrics have seen an increase in interest and developments over the years and have become a factory standard in authentication methods. Compared to traditional password entry methods, face and voice biometrics are faster performing. However, there are still security and privacy issues that needs to be addressed (Stokkenes, Ramachandra, & Busch, 2016; Trewin, et al., 2012).

2.2.3 Two-factor authentication

Despite the complexity of passwords, more often than not, they do not provide the highest level of security that is desired in computer systems. Two-factor authentication, also known as two-step authentication or multi-factor authentication, is a mechanism which is often used together with either passwords or biometrics to make the authentication process more secure. By implementing a two-factor authentication solution in a login system, common security threats such as Man-in-the-Middle (Schneier, 2005) and brute-force attacks are less effective (Aloul, Zahidi, & El-Hajj, 2009). Two-factor authenticators comes in different formats, either hardware or software. Nevertheless, they are used to generate a one-time-password (OTP) that will expire after a set limit of time. Examples of which includes smart cards, security tokens (code chips), or USB token, and OTPs received by email, SMS or application (see Figure 2.5). Two-factor authentication has been adopted to many digital daily life use cases, including financial, work and personal activities (Cristofaro, Du, Freudiger, & Norcie, 2013).



Google Authenticator

Google (surfingfan@gmail.com)
901 291

Google (hikingfan@gmail.com)
473 498

To: 732-873 Details

SMS with 732-873
4/14/20, 8:50 AM

Your security code is 273860. Happy Dropboxing!

Text Message

(a) (b) (c)

Figure 2.5 Examples of two-factor solutions: (a) code from security token, (b) code from the Google Authenticator app, (c) code from SMS.

3 Literature review

This study bridges viewpoints from human-computer-interaction, such as usability and functionality, and data protection, including GDPR and privacy. This section will cover and review literature of different topics regarding the aforementioned areas. The topics include social media, online services, and risk perceptions.

3.1 Online services

Digital technologies are essential in accessing online governmental services used in everyday life activities (Knowles & Hanson, 2018). Schehl, Leukel, & Sugumaran (2019) identified and meassured six online activites using older adults. The activities included browsing the web, viewing pictures and videos, writing e-mails, posting comments, banking, and shopping. The researchers found connections between demographics, including education, and online activites. Younger, higher educated men were more likely to succeed in instrumental activities (banking and shopping), while people with more cultural exposure were more likely to view multimedia. Social media and e-health was not addressed in the research, however.

In a study focusing on drivers and barriers in online shopping for older adults, the expectations, actions and issues faced when doing online shopping came to light. Generally, older adults are more confident in accessing traditional physical stores. Further, they tend to see online payment as more risky than phyiscal payment to another human being (Lian & Yen, 2014). As people are ageing, physical and cognitive abilities will decline, which will affect their computer skills (Knowles & Hanson, 2018). Lian & Yen (2014) found that adults who are experiencing funcational barriers are more likely to resist using online banking, which will in turn make them refuse shopping online. Furthermore, when the researchers compared a group of younger people to a group of seniors, 91.9% of the younger group had online shopping experience, while the seniors only issued 24.4%.

While the experiences of older adults in e-health is well document (e.g., Becker, 2004; Currie, Philip & Roberts, 2015; Flynn, Smith & Freese, 2006; Frennert & Östlund, 2016; Rockmann & Gewald, 2015; Tennant, et al., 2015; Xie, 2011), the following section will focus on their practices in social media and networking.

3.2 Social media

A substantial body of research has found that social medias are more often used by teens and younger adults than older adults. In a study conducted by Bowe & Wohn (2015) the researchers compared online media usage between two generations; those aged under 32 and those aged 32 or older. There were 2,032 total respondents in the study, and the researchers found significantly more people in the younger generation using social medias. Similarly, in a 2010 Pew report, the research center had collected data from 5 different age groups of American citizens: teens through adults aged 65+. The report showed that only 38% of older adults are using the internet, whereas teens and young adults make up 93%. Although Facebook was shown to be the most frequently used social networking site, they used Twitter as a measure of social media usage. They found people aged 18-24 to be the most frequent users of the media (37%), while only 4% older adults (65+) used the same service (Lenhart, Purcell, Smith, & Zickuhr, 2010). Another study used a subset of a bigger sample, focusing on 40 older adults between the ages of 65 and 91. The study showed that 45% of their participants used Facebook, 30% used Skype, and 8% Twitter. (Quan-Haase & Elueze, 2018).

In a study conducted by Hope, Schwaba & Piper (2014), they interviewed 22 older adults in the ages of 71-92. The researchers found that only 8 participants reported to be using social medias. Among the participants, 7 reported using Facebook and 1 using Twitter. Further, only three participants stated to post anything on Facebook, while two others said they were "lurking", meaning watching without posting. Furthermore, another American study was conducted recruiting older adults. The researchers analyzed 142 surveys answered by the participants, mean aged 71.64 years old. In the study, they divided the respondents into two groups: Facebook users (42%) and Non-Facebook users (58%). The researchers measured data regarding social satisfaction, confidence in technology and attitudes toward technology. The most significant finding was highlighted in the confidence in technology score. The Facebook users reported to have more confidence in their ability to learn new digital technologies than the non-Facebook users. Those who did use Facebook reported technology to have significantly more impact on their lives than the non-users (Bell, et al., 2013).

In Norway, 33% of people aged 65-74 are using social media daily or several times a week. Further, there are 17% of people aged 75-79 with the same social media activity. All other age groups, however, have a value equal to 53% or greater. See figure 3.1 for reference (Statistics Norway, 2018).

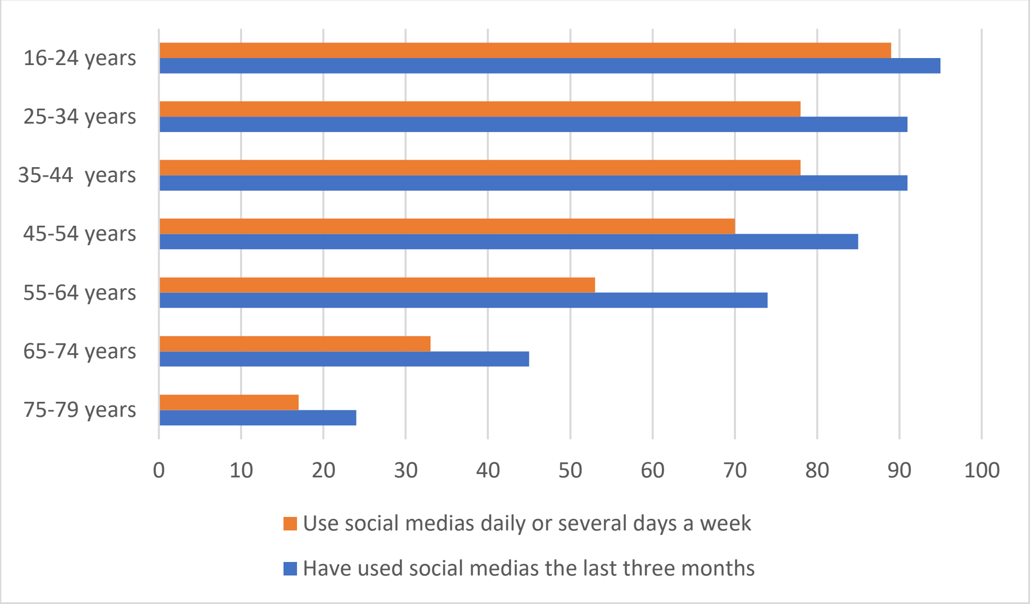


Figure 3.1 The Norwegian population's use of social media, sorted by age. 2018

Multiple studies show risks being introduced when using social medias (e.g., Nyblom, Wangen & Gkioulos, 2020; Lüders & Brandtzæg, 2017; Quan-Haase & Elueze, 2018). Researchers studying social media usage for Thai elderly identified six issues that can affect their everyday lives. These issues include violation, identity theft, lack of physical contact, negative impact on career, reduced health, and fake news publication. The researchers concluded that exposing information security is the major risk of social media usage, followed by media awareness (Nuchitprasitchai, Kilanurak, & Porrawatpreyakorn, 2020). Quan-Haase & Elueze (2018) identified privacy concerns among older adults in social media. According to them, the biggest concerns were unauthorized access to personal information, followed by information misuse, and then surveillance. In another study, older adults were interviewed to identify privacy and security concerns. The primary concern was to have their personal information sold or misused, resulting in reputational damage or public humiliation. The participants were asked of generational differences in privacy risks. They expressed privacy as a human right, which they learned growing up. Furthermore, when asked whether older adults are seen as attractive targets, their responses were mixed. Some stated that seniors are easier targets and more vulnerable, while others responded that their information is not useful enough (Frik, et al., 2019). Moreover, Frik, et al. (2019) categorized privacy and security management into two approaches: passive and active protection strategies. The passive strategies include being generally cautious, using online services with good reputation, and limit, or even avoid, the use of digital technologies. When approaching active protection strategies, the users must perform some actions to mitigate risks. Examples of active mitigating strategies are to use enhanced authentication methods, configure privacy settings, use protective software, and refuse to share personal information.

Similar to the protection strategies, social media usage has been categorized into the same two groups: passive and active. Passive users, also referred to as lurking, are very limited in interacting with and publishing content. They tend to consume what their online friends, groups and other people of interest are posting. Opposite, active users are much more interactive in social media and networking sites. Being an active user includes commenting, posting, and sharing to other people online (Hope, Schwaba, & Piper, 2014). Among older adults, women are more likely to use social medias and are more active than their male counterparts (Brewer, Schoenebeck, Lee, & Suryadevara, 2021; Parida, Mostaghel, & Oghazi, 2016). Some seniors choose to severely limit the use of or stay away from social medias entirely. Negative attitudes towards social networking includes lack of time and interest, physical and psychological impairments causing pain or fatigue, and demographic barriers including language and internet accessibility (Nimrod, 2014).

4 Methodology

The study adopts a qualitative method, individually interviewing the participants. The interviews were conducted to collect data on the experiences of older adults, in managing privacy and data security using online services. Rather than using a “question and answer” format for the interviews, or questionnaires, semi-structured interviews were used.

4.1 Ethical Approval

Before recruiting the participants, approval from The Norwegian Centre for Research Data (NSD) was obtained. During this process, study-related documents, including interview guide, information sheet, consent form, and data management methods had to be submitted.

4.2 Recruitment

After approval, an invitation was distributed via Seniornett, an organization focusing on helping elderly people in different digital activities. The invitation was distributed on February 12th, 2021. It was also published through the organization’s weekly newsletter.

Interested members were asked to contact the researchers, and questions about the study were answered via mail or phone calls. After members expressed their interest, the information letter and consent form were sent to them, which they would read and sign for participation. Due to the effects of the COVID-19 pandemic, meetings could not be arranged in person, and the consent form had to be replied by mail. Knowing that electronic signatures would cause problems for some of the less experienced users, a guide was created on how to sign PDF documents using Adobe Acrobat DC Reader[1], and how to set the program as default application for PDF handling. The document is located in Appendix A. After receiving their signatures, individual interviews were scheduled. Twenty-three members were recruited to participate in the study.

4.3 Data collection

The interviews focusing on collecting data about participants’ awareness, experience, knowledge, concerns, and strategies in relation to data security and privacy. Throughout the interviews, the goal was to find out about the interviewees’ everyday privacy and data security management. Furthermore, the focus was on their protection towards passwords and cookies when carrying out online activities. These acts include using social media,

[1] https://get.adobe.com/uk/reader/

visiting websites, doing online shopping, and using online banking services.

The interview guide was important seeing as semi-structured interviews were performed. The guide would help structuring the interviews in a way so the interviewees would not get too off track, although they were allowed to speak freely of their experiences. In cases of digressions, the guide could help the interviewer and interviewee to recover. Furthermore, three main categories were identified as a template for the interview guide: background, data protection and passwords.

In the first category, the following attributes about the interviewee wanted to be answered or discussed: age, gender, employment, what devices they use, social media and online service usage, online privacy, and GDPR. This would help in getting a *picture* of their online profile and would serve as the foundation for the remainder of the interview. The next category, data protection, would elaborate on their privacy literacy defined in the previous listing. The data protection category would focus on their experiences with, and thoughts on cookies, concerns, and protection strategies. Additionally, the last category adds to the protection strategies, as it focuses on the participants passwords. This includes habits when creating passwords, methods of authentication, how they manage passwords, and their experiences with online banking.

Looking at the three categories, sixteen questions were defined. Within the first category, five questions (Interview guide question 1-4 and 8) were outlined. The next category fitted three questions (Interview guide question 5, 6 and 7). The final category included seven questions (Interview Guide question 9-15). While the last question (Interview guide question 16) did not fit into any category, it served as debrief. Here, the interviewee could follow up on any of the questions asked during the interview, add a statement, or simply share some ending thoughts - rounding up the interview. Below, the Interview guide questions are listed.

1. Tell about yourself (including age, work situation, and what devices you use).
2. Do you use any social medias?
3. What other websites do you use?
4. Do you have any thoughts on your online privacy?
5. Do you have experience with cookies?
6. Do you feel comfortable and safe when using the web?
7. Do you know how to protect your data?

8. Do you know about the General Data Protection Regulation (GDPR)?
9. What is your thought process when making a password?
10. How do you remember your passwords?
11. Have you ever heard of a password manager?
12. What do you know about two-step verification?
13. Have you used BankID[2] for login?
14. Do you usually log out of your online accounts manually?
15. What are the biggest issues with passwords in your experience?
16. Any final thoughts?

The interviews were conducted during February through March 2021, the first interview dated February 15th and the last dated March 11th. Most interviews were done over phone calls as the participants was comfortable using this method. There were some exceptions where the interviewees wanted to participate online, feeling more comfortable seeing the face of the interviewer. In these cases, Zoom was used as the tool of communication. The interviews were recorded, and the interviewer took notes during the interview. While taking notes during an interview can seem distracting, it helped in paying attention to what the interviewee was saying, and to structure the information given for later reference during the interviews.

The equipment used to record the interviews was a Huawei computer running Windows 10 and a Blue Yeti USB Microphone. Because of GDPR, recording voice calls without consent is illegal, which have led to telecommunication providers disabling the option to record calls. Hence, the calls for the interviews were recorded using the USB microphone and the speaker option on the caller's phone. In cases where Zoom was used to conduct the interviews, the sessions were recoded using the built-in audiotape function in Zoom. After each interview had been recorded, the file was transferred to a different storage media.

When the interviews were completed, seventeen hours of interview data had been collected and analyzed. The average length of the interviews was forty-four minutes. However, the length of the interviews varied; the shortest interview was twenty-six minutes and the longest was eighty-eight minutes.

[2] https://www.bankid.no/privat/

4.4 Data analysis

A thematic analysis was conducted. Any disagreements concerning coding and themes were resolved by discussion with the supervisor. At the stage of analysis, some participants were contacted to clarify answers they provided during the interviews.

Using the audio files and notes from each interview, the data was extracted to an Excel spreadsheet for more readable and comparable information. In doing this, the information was easily visualized using functions to sort the data and inserting charts.

4.5 Pilot

A pilot interview was conducted with Siri Kessel, who used to work as a professor at OsloMet before retiring. Now, she is volunteering at Seniornett, working with management. In the interview, feedback was collected about the invitation letter, information sheet, and the data collection method. After going through the information sheet, Siri proposed some suggestions of improvement, like precising the more open question. An example of such is in Interview Guide question 1, which was very broad, and resulted in adding a specification of what data we wanted to collect. Another suggestion was in the invitation letter. Here, we agreed to conduct the interviews primarily by phone, as it is more accessible than certain technologies (e.g., Microsoft Teams or Zoom). Furthermore, she stated the importance of participation to make way for more research being done in this field.

Seeing as Siri is a member of Seniornett, she often explained the recruitment process. The feedback was used to make changes before the recruitment and the conduction of interviews.

5 Results

5.1 Participants

In total, 23 participants were part of the study, including 14 males and 9 females (see Figure 5.1). The participants' identity will be protected, and they will be referenced as P1-P23. Their age ranged from 69 to 83 years. The mode was distributed between four values, as they all had the frequency of three, the values being: 69, 73, 75 and 83. Figure 5.2 The age of each participant (P1-P23). The horizontal line indicates the mean age of all the participants. The participants claim to have at least 15 years of internet use experience. 10 of the participants stated that they started using computer systems and the web during the 1990's or as early as the 1980's. This was often related to the requirement of using computer systems in their jobs, commonly information technology, accounting, and research.

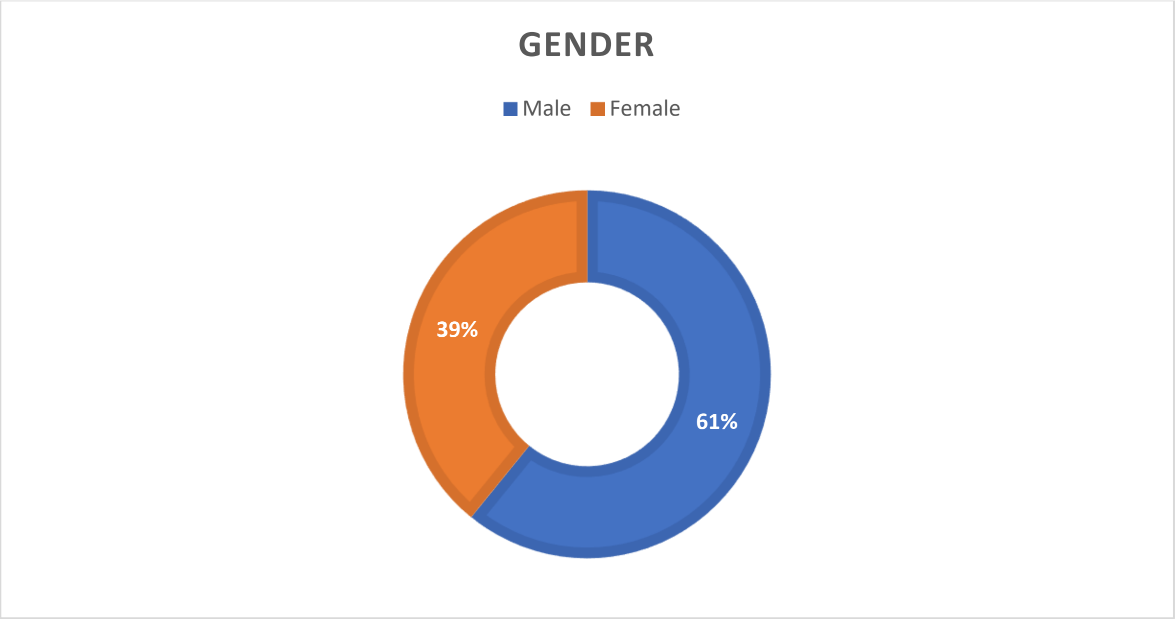


Figure 5.1 The gender distribution among the participants.

The participants' social media usage was somewhat varied. The majority of the participants reported that they were using Facebook regularly. There were three participants who said they did not use Facebook, two of them did not feel the use for Facebook, as they were using LinkedIn regularly instead. Only one participant stated that they were not using any social media at all. Most of the participants using Twitter were also using Instagram. Three reported that they were using Snapchat, however some said they had been using it previously but did not like the concept of pictures and chats disappearing after a short period of time. Others reported that they would like to use Snapchat more to connect to their family, especially grandchildren, who tend to use it actively. The participants' social media usage was categorized into two, active and passive. The active being those who tend to post on one or more social medias regularly, and the passive being those who tend to watch content but not post anything themselves. Figure 5.3 The distribution of social media services among the participants, including Facebook, Instagram, Twitter, LinkedIn, and Snapchat.

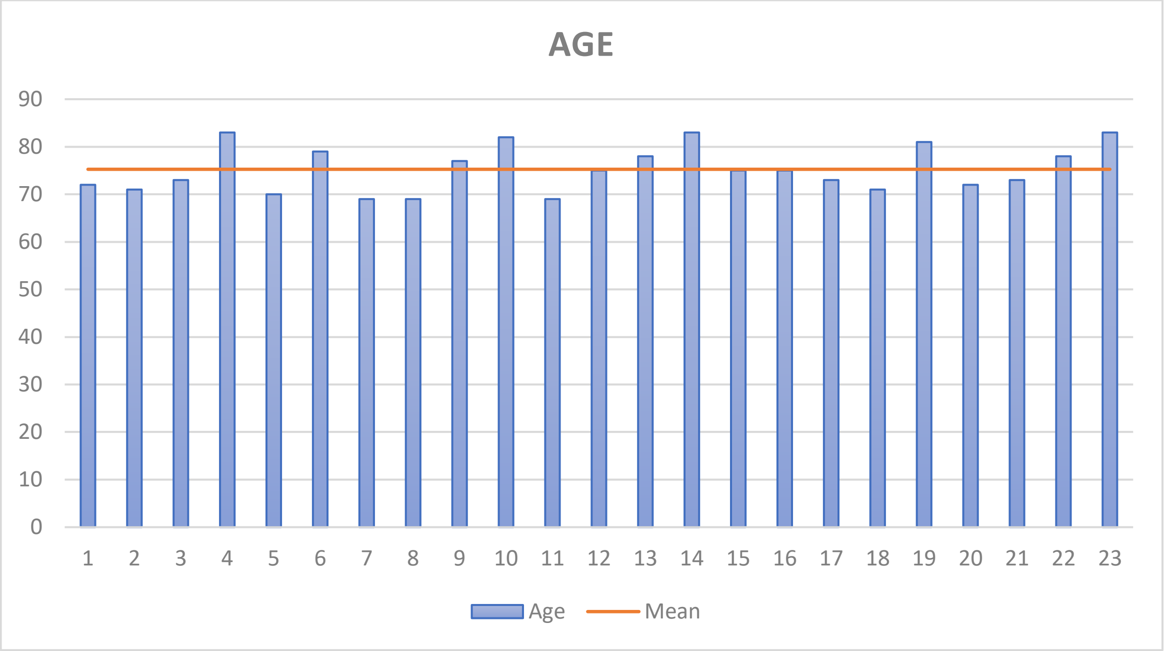


Figure 5.2 The age of each participant (P1-P23). The horizontal line indicates the mean age of all the participants.

Furthermore, the participants have been using a set of communication services. Some stated that they started using these technologies during the COVID-19 pandemic to connect with family, friends, committees, or part time labor. The most common technology of which is Zoom, followed by Skype and WhatsApp. Usually, the participants are familiar with more than one of these services. In the case of them using e.g., both Zoom and Microsoft Teams, they claim that Teams is harder or more cumbersome to use than the counterpart. Figure 5.4 The distribution of other communication services among the participants, including Zoom, Skype, WhatsApp, Teams, and Line.

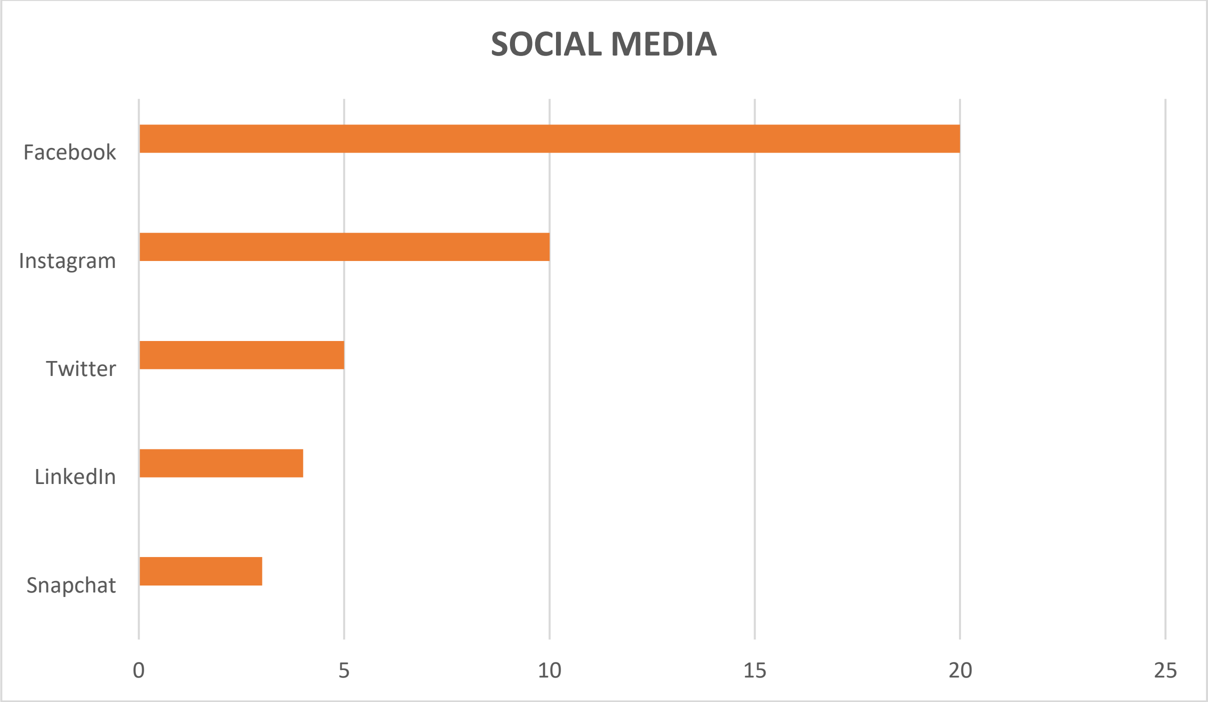


Figure 5.3 The distribution of social media services among the participants, including Facebook, Instagram, Twitter, LinkedIn, and Snapchat.

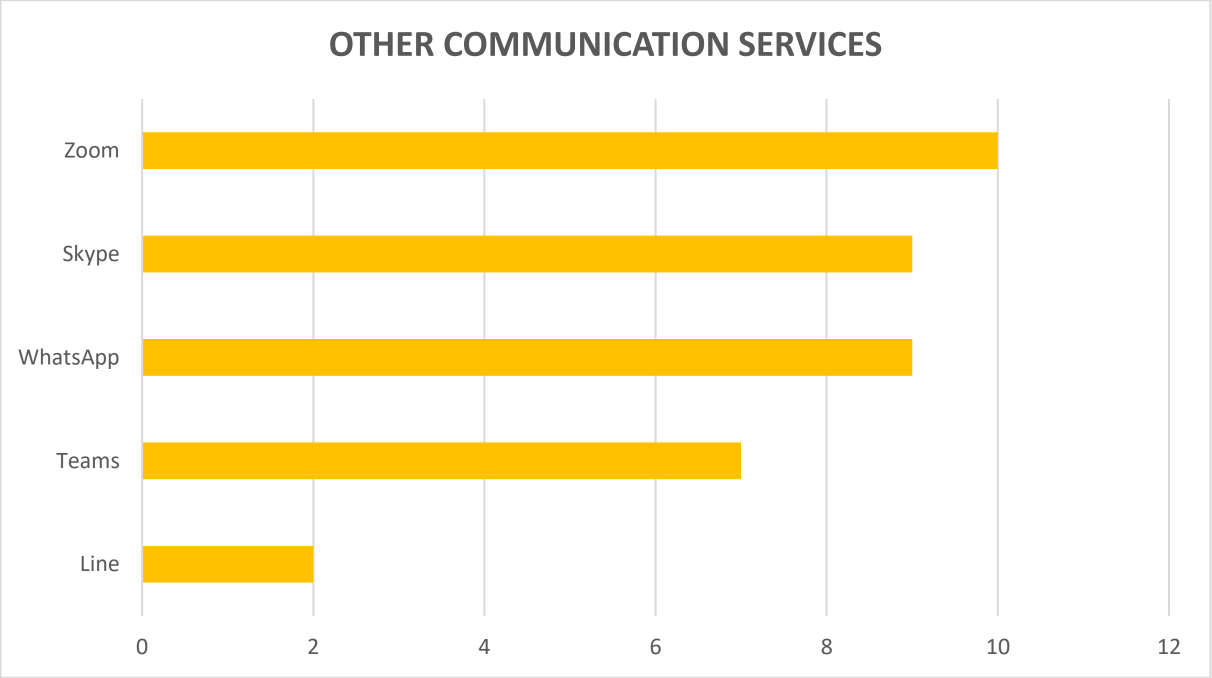


Figure 5.4 The distribution of other communication services among the participants, including Zoom, Skype, WhatsApp, Teams, and Line.

All the subjects use online banking services for daily tasks, including paying bills, manage accounts and deal with stocks. It is an imperative service in the everyday life of Norwegian inhabitants. Most participants stated that they are required to use the same login procedure for other, similar services, including pension, e-health, taxing, and to complete purchases while online shopping. Moreover, 17 participants tend to do online shopping, specifically because of the effects of the pandemic. The remaining 6 does not do online shopping at all. Some stated that they prefer physical stores more and would like to support their local stores rather than buying from a major industry. The subjects that are doing online shopping, however, were generally happy about the ease and accessibility. Although, some have stated their concerns about it, which will be focused on in a later section.

The participants all reported that they are reading online newspapers. Some preferred reading the newspapers on paper as it felt more comfortable to them and often reduced the strain on the eyes which would come from reading it on a screen. The majority stated that reading it on a larger screen like a tablet or computer was the preferred method. Furthermore, the participants reported using devices including smartphones, tablets, laptop and desktop computers (see table 5.1). Ten of whose were using one or more Apple devices, mainly iPhone, iPad, and MacBook. The others claim to use smartphones and tablets manufactured by either Samsung or Huawei, and use Windows computers running Windows version 8 or newer.

Table 5.1 Devices owned by the participants.

DEVICE	NUMBER OF PARTICIPANTS
COMPUTER	23
MOBILE PHONE	23
TABLET	15
WEARABLES	2

5.2 Passwords and authentication

Passwords was found to be challenging for all the participants. From the interviews, 3 main challenges were identified: to remember the passwords, making the passwords unique, and changing the passwords. Lastly, one participant named identity theft as a direct challenge to passwords. Below, an overview of the challenges is shown (see Table 5.2).

Table 5.2 The main challenges with passwords.

CHALLENGE	NUMBER OF PARTICIPANTS
HARD TO REMEMBER	12
THE UNIQUENESS	5
TO CHANGE THEM	5
IDENTITY THEFT	1

12 subjects reported that it is hard, or even impossible to remember passwords, and see this as the biggest issue. Next, there were 5 people saying the uniqueness of passwords is the most challenging. There are password composition requirements, like using upper- and lower-case letters, numbers and symbols, and a required password length in characters. This is just one part of the challenge. Further, they are asked to use a unique password everywhere they create a new account. 5 participants stated that changing their passwords was the biggest issue. This is closely related to the previous challenge, as they often manage to create a unique password but are then asked to change it after a period of time. Participants also found the experience of changing passwords *cumbersome* and *frustrating*. Out of all the participants, 15 reported that they write their passwords down. This is often done on a note on their desk or in a file saved on their personal computer. Majority of the time the passwords are noted in a book which can be carried around everywhere they go. Some of the participants stated that they write down their passwords although they are aware of the risks of doing it, while saying there is no other way for them to remember the passwords otherwise. A major issue is when they are asked to update their passwords, but do not have access to the book, note or file. This requires them to remember the new password until they can access their password media. The remaining seven reported that

they do not need to write down their passwords; two of whose said they can remember them with no aids. Five participants claim to use a password manager, such as LastPass[3], Norton Password Manager[4], or Password Safe[5] (see Figure 5.5).

The participants who use a password manager reported that they all have been using them for more than 2 years, and up to 10 years. Some web browsers such as Google Chrome[6], Mozilla Firefox[7] and Microsoft Edge[8] have built-in password managers, which two participants reported to have used. These tools have similar features to the state-of-the-art password managers, including generate a password for the user, save the new password, and remember existing passwords that have previously been used. Eighteen participants did not use a password manager. Four of the participants were interested in using a password manager, and three had already tried using one but found them to be too complicated to learn and use.

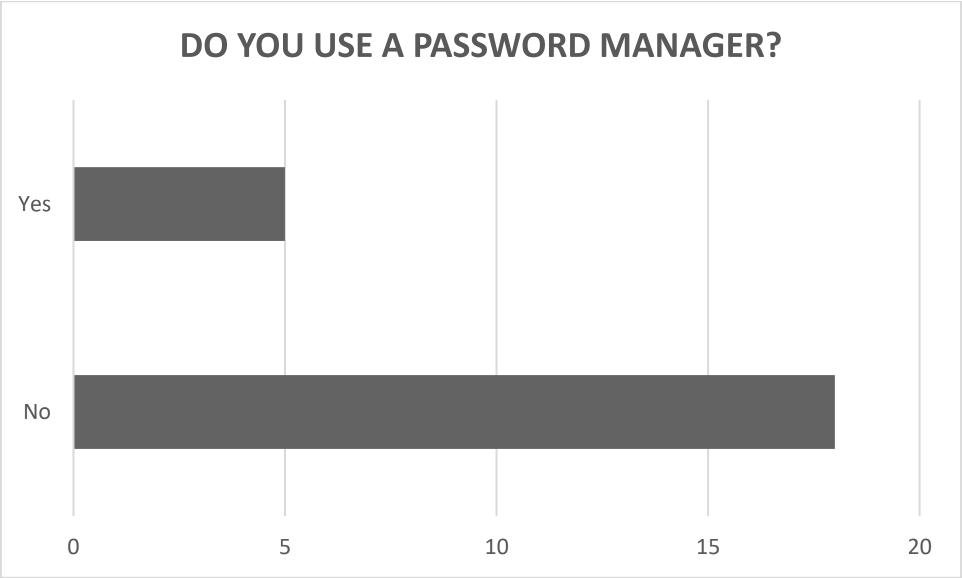


Figure 5.5 The response from the participants when asked if they use a password manager.

As previously mentioned, all the participants were using online banking services, which meant they were familiar with two-factor authentication. The participants found it challenging and tedious to use at first but got more comfortable after more frequent use.

[3] https://www.lastpass.com/how-lastpass-works
[4] https://my.norton.com/extspa/passwordmanager
[5] https://pwsafe.org/
[6] https://passwords.google.com
[7] https://www.mozilla.org/en-US/firefox/lockwise/
[8] https://nordpass.com/blog/view-edit-delete-saved-passwords-edge/

When identifying and logging in to online banking services, the participants used a physical code chip and/or an application displaying a one-time code. Out of the 23 total participants, 16 reported to be using the code chip and 11 reported using an application (see table 5.3).

Table 5.3 The participants' response to what two-factor authentication they were using.

METHOD	RESPONSE
CODE CHIP	10
ONE-TIME CODE APPLICATION	5
BOTH	6
DID NOT SAY	2

The subjects had a common idea of protecting health and economic information, stating that two-factor authentication makes them feel *safer* and *more reassured*. Despite the authentication process being more time consuming due to the extra step, the participants feel that this solution is *well-established* and *works well*. However, not all participants shared the same opinion. Sometimes it seemed as if the authentication was excessive, and not always needed.

"Two-step authentication is often more effort than what it is worth" (P12).

Generally, two-step authentication is used for online banking service. However, for other services including shopping and telephony, it is often integrated but not necessarily needed in all cases.

"Generally, two-factor authentication works well. Sometimes it is used in applications where I do not think it is necessary" (P19).

Only one participant responded that their preferred authentication method was biometrics. 8 participants were using biometric authentication for services such as Vipps[9] and mobile banking, and for unlocking mobile devices and laptops. When asked about what authentication method could replace passwords, 8 mentioned biometry as a solution and 2 mentioned BankID to be a more commercially used solution for login. Furthermore, seeing as

[9] https://www.vipps.no/

the participants were older adults, a common problem was recognition of fingerprints. Their fingerprints tend to be *out-worn* and hard to recognize.

5.3 GDPR and Cookies

Seventeen participants reported that they had heard about the GDPR and had an idea of what it means, often when seen in context, but did *not know the details* (see Figure 5.6). While P9 stated that they *enjoy openness online as it provides safety*, P13 thinks *we might need something even stricter*. One of the participants had learned about GDPR at work and was the only one who could explain it in detail. P17 reported that they had used an information removal service to remove some content from the media, saying *someone posted a picture of me online which I reported, as I did not consent. The individual was forced to remove the post*. In Norway, the Norwegian Centre for Information Security (NorSIS) is a key organization for deleting data, offering services such as slettmeg.no[10] and nettvett.no[11]. These services enable all users to delete unwanted data online and provide information regarding each individual's privacy.

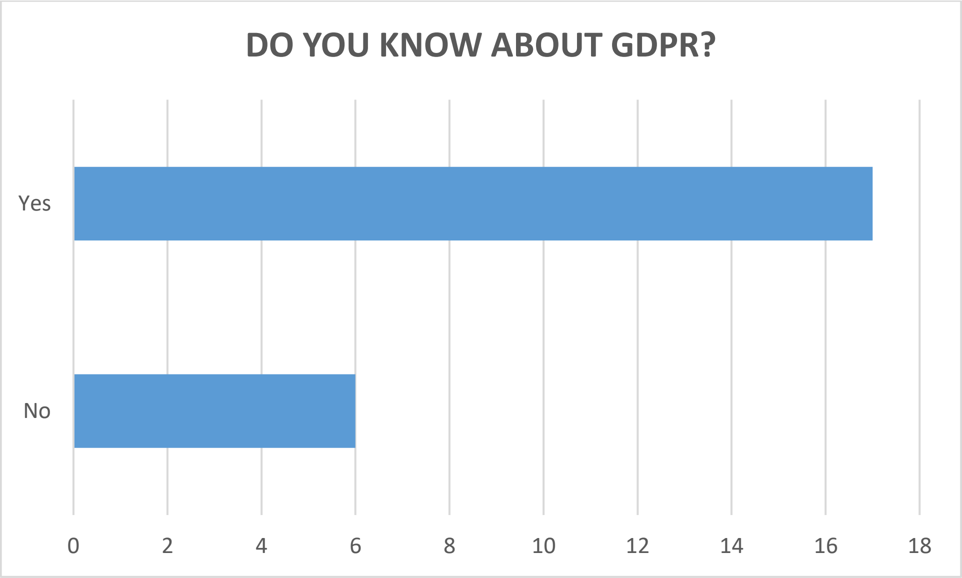


Figure 5.6 The response from the participants when asked about GDPR.

Regarding cookies, the participants had different behavior and approach towards cookies (see Figure 5.7). Seven felt like they must accept in order to proceed, saying they feel *pressured* to do so. Additionally, four blindly accept, as they do now what it means to accept.

[10] https://slettmeg.no/

[11] https://nettvett.no/

Conceiving information about cookies tend to be a challenge. One participant, P23, stated that they found the cookie information to be *a hassle to read about*.

"To use the website, I have to accept. The information about cookies is hard to read" (P11).

"To proceed I have to accept. Changing preference is too time-consuming" (P22).

Moreover, twelve participants tend to change preference. Seven of them reported to sometimes accept cookies but would otherwise change preference. In addition, they stated to accept when visiting *familiar* websites, however changing preference can be *complicated* and *take some time*. P19 said *I tend to change preference. If I do not have time to do so, I* accept. The last five would always change preference or reject whenever possible, including P21, stating to *decline or block whenever I can. Otherwise, I will change preference*. P13 however, looks to give *full access or limited access*, depending on what website they are visiting.

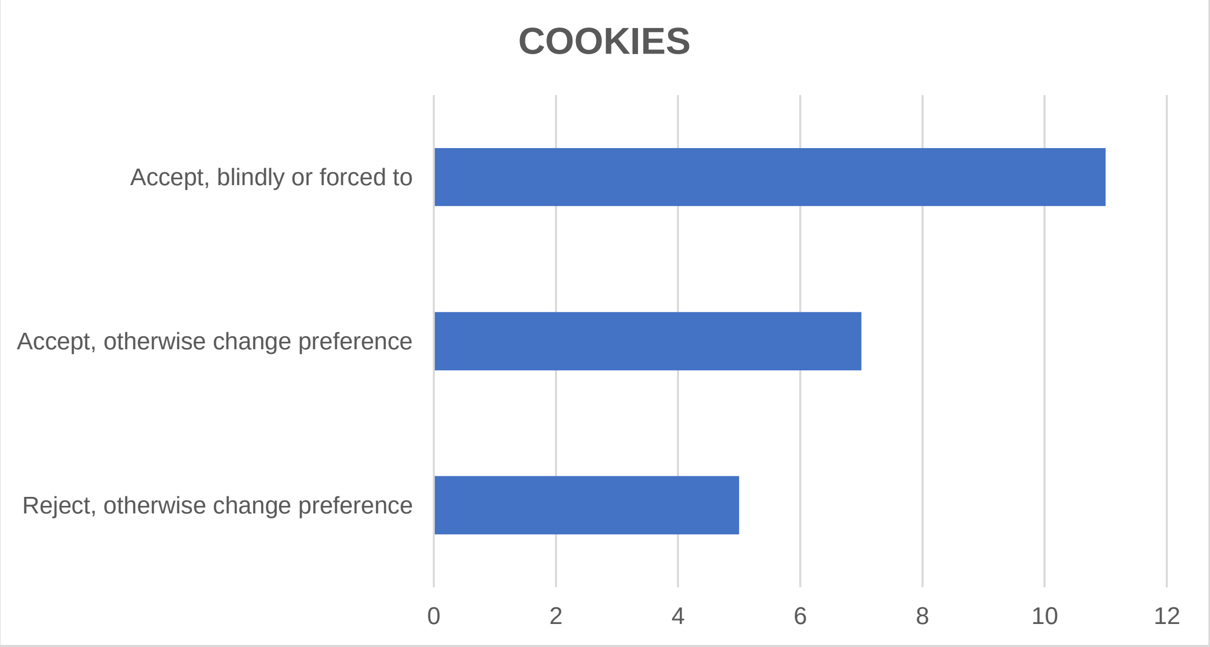


Figure 5.7 The distribution of how the participants approached cookies.

5.4 Concerns and protection strategies

The interviewees were asked whether they had any concerns, if they felt safe, or even comfortable using the internet. Ten subjects responded that they felt relatively safe; however, they did not feel comfortable. They reported to be aware of the possible risks and threat actors in the online world. Some of the risks include leaking of personal information, phishing, online surveillance, identity theft, and online fraud. Although P2 *feels pretty safe* they are still aware of *information leaking, being sold and conveyed.* They further stated that *things are happening 'behind the scenes'* meaning organizations are taking actions the users are not aware of nor informed about. Another concern stated by P1 and P22, resolves around major companies such as Facebook and Google – *or third parties collecting more information than necessary*. Regarding threat actors, the participants were aware about the possibility of hackers and other cybercriminals stealing their information.

“*I know that it is dangerous online, and I know about hackers and people who would like to do harm*, while not identifying themselves as a target; *for me, it is not that dangerous, as I do not feel exposed. I just need to be cautious of the websites I visit*” (P23).

Simultaneously, three participants reported they had been targeted as victims for cybercrimes. One of which found out from a Microsoft report saying their account had been hijacked from two separate IP addresses located in Asia. Despite this, they stated to still feel safe because of their long experience using online services.

Only a few participants responded to have no concerns, saying *I have no concerns, as I do not have anything to hide* (P10). Further, P4 responded *I am optimistic, and I have no concerns. Although, I am bit quick to click on some links.* However, others were more worried about the risks of using online services or did not feel safe using them.

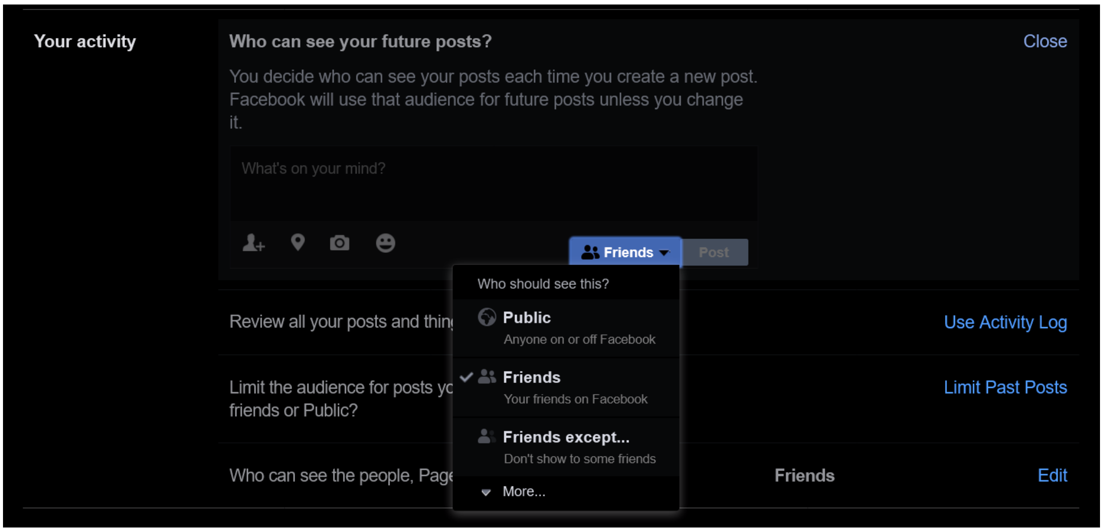
“Yes, I do feel surveilled when using the web. It is possible for them to see what I've been searching for” (P17).

“No, I have no worries, but I do not feel safe either. And I am extremely careful” (P9).

Furthermore, some participants feel more helpless than others when using online services. They responded to *rely on help from others* (P18) and *lack knowledge about security on websites* (P21). Although some found it harder to protect their privacy, the participants reported using various protection strategies.

One of the most basic protection strategies when using online services, reported by the participants, was using etiquette in technology. Etiquette in technology elaborates on the idea of being generally cautious when using a computer, including being selective about where to shop, using familiar and trusted websites, not sharing personal, financial and health information, and checking before clicking links. One of the participants defined this as the traffic rules of the internet. When you are navigating the internet, you are in the driver seat. This means that there are precautions that needs to be considered, making accidents less likely to happen.

Moreover, eight participants reported to be checking and changing privacy settings regularly. Privacy settings are quite different depending on what service you are. In social media there are options to choose whom you want to share your information with. Facebook has the option to share to “friends”, “public” or a defined selection, Instagram has the option to toggle a private account, limiting the amount of people who can view your posts, and Snapchat has a GPS function which can be turned off (see Figure 5.8-10).



Your activity

Who can see your future posts?

Close

You decide who can see your posts each time you create a new post. Facebook will use that audience for future posts unless you change it.

What's on your mind?

Friends ▾ Post

Who should see this?

Public
Anyone on or off Facebook

✓ Friends
Your friends on Facebook

Friends except...
Don't show to some friends

▾ More...

Review all your posts and thin

Use Activity Log

Limit the audience for posts yc friends or Public?

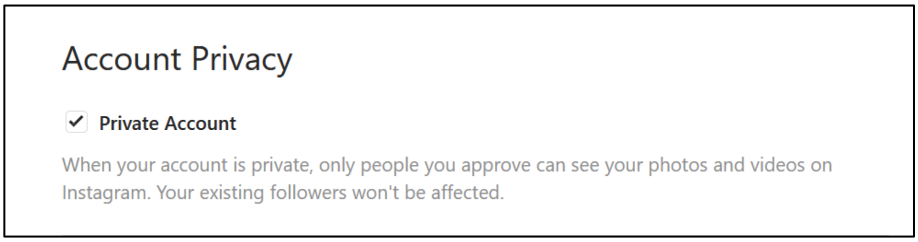
Limit Past Posts

Who can see the people, Page

Friends

Edit

Figure 5.8 Screenshot. In the privacy settings in Facebook, the user can select who will see what they are posting.

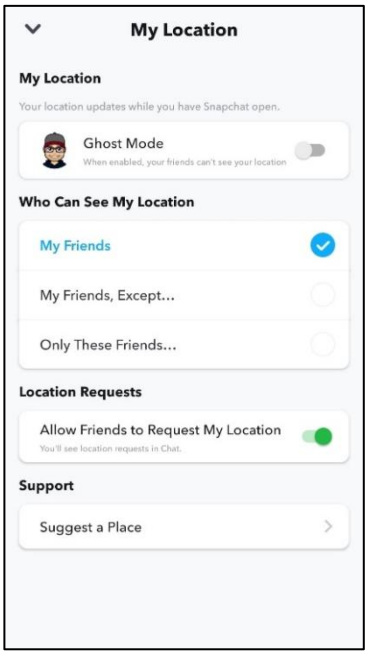


Account Privacy

☑ Private Account

When your account is private, only people you approve can see your photos and videos on Instagram. Your existing followers won't be affected.

Figure 5.9 Screenshot. In the privacy settings of Instagram there is an option to choose whether the accounts are private or public.



My Location

My Location

Your location updates while you have Snapchat open.

Ghost Mode ○
When enabled, your friends can't see your location

Who Can See My Location

- My Friends ✓
- My Friends, Except... ○
- Only These Friends... ○

Location Requests

Allow Friends to Request My Location ●
You'll see location requests in Chat.

Support

Suggest a Place >

Figure 5.10 Screenshot. The privacy settings in Snapchat lets the user opt to share their location and whom they are sharing it with.

Similarly, online services such as shopping, newspapers and food ordering often ask for the user's location to recommend pick-up points, close restaurants or similar. The participants who reported to change privacy settings most often *turn them off, and on turn a selection if needed*. Furthermore, four participants responded that they check the URL of websites they are visiting, using an elimination method to see whether the website is safe or not. The most common approach they are using is to look for HTTP or HTTPS. The four participants were aware that the S was an abbreviation for secure. Another approach used by the participants was to look for the padlock-icon next to the URL. Although they did not know all the details regarding the symbol, they recognized it as more secure.

"I've learned that I need to look for the S in 'HTTPS' and padlock when I'm visiting websites, because it has to do with security… I was once managing a subscription when I almost got fooled, and that was because I wasn't paying attention to the address in the browser" (P4).

Moreover, eleven participants reported to regularly use anti-malware or anti-virus software. Although used for the same purpose, the participants were familiar with a range of different software, the most popular being Norton[12]. Other software used by the participants include Windows Defender[13], Malwarebytes[14], McAfee[15], and AVG[16]. Within the same group, one reported to be using a dedicated advertisement blocker, while another participant reported using a URL scanner.

[12] https://us.norton.com/
[13] https://www.microsoft.com/en-us/windows/comprehensive-security
[14] https://www.malwarebytes.com/
[15] https://www.mcafee.com/en-gb/index.html
[16] https://www.avg.com/en-ww/homepage

"I have a folder in my browser named 'Check suspect websites', and it contains three-four tools which lets me search for different addresses I find suspect" (P16).

Three participants responded they tend to visit the Data Protection Authority's websites to look for updates and help, if needed. One of the three also reported to get help from the Consumer Authority. Lastly, four participants identified trespassers in mail services by looking at spelling, bad wording, formulations, and overall use of language. They stated that these factors could easily recognize the legitimacy of the sender, the next action would be to delete the mail if it seemed suspicious. See Figure 5.11 for an overview different protection strategies used by the participants, a more comprehensive review of the strategies is located in Appendix B.

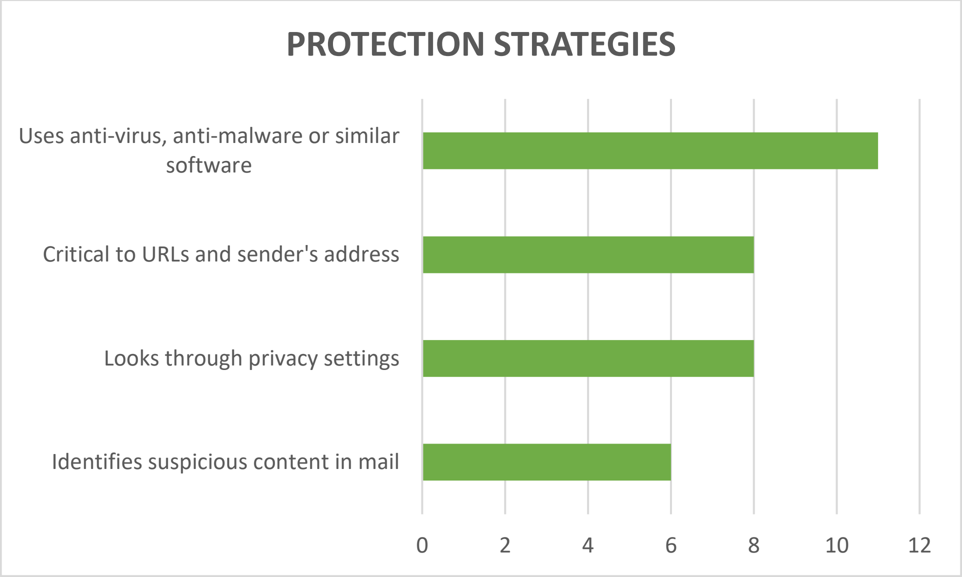


Figure 5.11 Overview of the different protection strategies used by the participants.

When participants were asked whether they actively logged out of their accounts after use, their responses showed that they handled their social media accounts and their banking accounts quite different. Although P7 *equate social media and banking accounts*, the majority does not care about their social media accounts. The reasons mainly being that *I am not interesting* nor *have much to hide*. However, they considered their personal finances and health information especially important to protect. Table 5.4 shows that twenty participants often or always log out of their online banking accounts while only three tend to do the same for their social media accounts. Furthermore, P5, P17 and P18 did not know how to log out of their social media accounts when used on either a mobile device or a computer.

Table 5.4 Number of participants who actively logged out of their accounts after use.

FREQUENCY	SOCIAL MEDIA ACCOUNTS	ONLINE BANKING ACCOUNTS
ALWAYS	2	11
OFTEN	1	9
SOMETIMES	3	1
NEVER	14	0
DID NOT SPECIFY	3	2

5.5 Suggestions

After reflecting on their own knowledge and protection strategies, the participants expressed their wishes and suggestions to learn more. This section focuses on suggestions for supporting them to further protect their privacy and data security.

Throughout the interviews, the interviewees mentioned using YouTube as a platform to seek information and find instructional videos. In addition, they highlighted information and instructions from the government and authorities for older adults.

> ***"I think that the directorates, ministries, and authorities should give more attention to what we have been talking about [online privacy and security], especially for the older people. But not only the seniors, the entire population could have benefit. Maybe they could make some aids and instructional videos or recommend one or three password administration applications" (P2).***

Further, they wanted courses on different levels, either face-to-face or online. Having courses covering the basics of digital technologies would get more people interested in using them and learn more about protecting their digital life. Only covering the basics would still be beneficial to more experienced users, as they could pick up something they did not know beforehand.

"Let's have a course for dummies and say, 'we are all idiots - some more than others - but we can do this together.' At least get everyone on a level where they can enjoy using a tablet" (P21).

Regarding courses, there were suggestions of having one-to-one interactions, as it would enhance the learning experience. Additionally, this would help better conceiving the information being given. Moreover, the participants wanted courses on hardware and software they were already familiar with. Getting further knowledge on the technologies already being used would be more efficient then spending time learning something they have no relation to.

"I wish that things were more facilitated for older people, in a better, more patient way. I decided to go online many years ago, which have really helped me in recent years." (P9)

"I miss having more courses for Mac. I bought my Mac first when I retired as I wanted to start studying. There were not many people who could help me, as the focus was on using [Windows] PCs" (P18).

Although some participants were familiar with changing privacy settings, others wanted a thorough introduction to both cookie and privacy preferences. Furthermore, participants commented that online services should provide better support for privacy and data security protection.

"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).

6 Discussion

Compared to previous literature, this study has found much different results regarding online services, privacy, and data security. Researchers have found limited use in social media for older adults (Bell, et al., 2013; Lenhart, et al., 2010; Quan-Haase & Elueze, 2018). However, the participants in this study showed very frequent use of social media, as all but one participant was using social networking sites regularly. Nimrod (2014) found *the lack of time* and *users not being interested* to be the main constraints to why older people choose to opt out of social media and digital technologies entirely. The findings in this study show support to this claim. Five participants reported that friends or family members have opted out of social media usage due to:

- the lack of **interest** in learning and using such services, and
- the lack of **time** in learning and using such services.

This study also indicates that older adults are more critical towards the use of health and financial information services than with social media and networking. This is demonstrated by the number of participants actively logging out of their online banking accounts, compared to the low number of active log outs in social media (see Table 5.4).

In terms of protection strategies, the passive and active strategies indicated in the findings are similar to the strategies identified by Frik, et al. (2019). However, the participants in this study were more knowledgeable about active protection strategies than the ones in the aforementioned study. Examples include physical security, and removal of unwanted content. Furthermore, the same researchers discovered that older adults often experienced usability issues when mitigating data security and privacy risks. Similarly, the participants in this study reported password managers to be complicated, changing privacy settings to be time-consuming, and changing cookie preferences to be cumbersome.

Furthermore, Knowles & Hanson (2018) expressed the users' negative attitudes towards online services such as banking and shopping. Similar to what the authors found, the participants in this study preferred the face-to-face interaction which is achieved when visiting physical stores. Ethically, people often want to support their local stores, which distances them from online shopping.

6.1 Limitations

There are several limitations to this study. First and foremost, the study has a small sample size of 23 participants. Although there is no clear answer to what a *good* sample is for qualitative research, Dworkin (2012) suggests a number between 5-50 participants, and recommends 25-30 as a minimum. This shows that the study would benefit a bigger sample of participants.

Furthermore, the selection suffered from convenience sampling. All the participants were recruited from one and the same organization, Seniornett. The organization focuses on improving the knowledge and IT skills of older residents, meaning the collection of participants should be better equipped than the general older population. Moreover, there were few requirements for participation. The participant needed to be 65 years old or older, and had to be using at least one digital technology or online service. This resulted in little knowledge about the background, computer skill, and privacy understanding of the participants.

6.2 Future work

There is much needed further investigation and research to be done in future study. Because of the current small number of participants, more participants need to be recruited. In the recruitment process, people with varying technical knowledge and social media non-users who are less literal in data protection and risk management, must be considered. Additionally, the sample must include participants who have previously used digital technologies, either through work or for personal use, but have decided to opt out of using different online services. In doing this, the following questions could be answered:

- Do they avoid using online services due to risks?
- How has training affected their understanding and strategies for privacy and data protection?
- What usability and accessibility challenges have they experienced in privacy and data protection?

Further, this study would benefit approaching a different method. Mixed methods, or multimethodology, combines the qualitative and the quantitative methods (Shorten & Smith, 2017). The quantitative methods would enable the use of surveys and questionnaires, which would provide more statistical data. However, semi-structured interviews would still be conducted for gathering qualitative data. By using the mixed method approach, it would increase the number of people participating in the study and impact the research in collecting more representative data of older adults.

7 Conclusion

The global pandemic has introduced a need for older adults to use online services that they were previously not utilizing. As this user group are turning their attention to technology, more risks have been introduced into their lives. As previous studies suggest, the likings and preferences of the older population need to be addressed in the process of designing new products (Frik, et al., 2019; Quan-Haase & Elueze, 2018).

In this master project, semi-structured interviews have been conducted to understand the experiences of older people regarding privacy, authentication and risk management in everyday online services.

The findings in this study show that the participants are generally aware and knowledgeable of risks. As a result, they have developed strategies to protect their privacy and digital data. This indicates that older adults in this study are better equipped in digital technologies and security than what the literature shows (Bell, et al., 2013; Brewer, et al., 2021; Hope, Schwaba, & Piper, 2014; Nyblom, Wangen, & Gkioulos, 2020).

Based on the literature (e.g., Inglesant & Sasse, 2010; Marky, et al., 2018; Renaud & Angeli, 2009) and the responses of participants in this study, passwords are found to be challenging. However, there are options to replace the traditional passwords that are used today. The participants reported solutions including biometrics, PIN and BankID as a replacement to password. Although 8 participants were in favor of biometric authentication, some reported usability issues, especially regarding fingerprints. The participants report difficulty in using fingerprint sensors due to wrinkles. Moreover, users are still anxious and in lack of trust in using biometric authentication methods (Andrew, et al., 2020), making it a less optimal design for older adults.

The results in this study indicate that instructions, adequate training and well-designed technical solutions is important in understanding and mitigating risks in privacy and data protection, which further contribute to the acceptance and adoption of digital technologies for older adults. Moreover, the findings have shown that people who are interested in learning about new technologies can indeed learn it. Similar to the identified literature (Andrew, et al., 2020; Frik, et al., 2019; Knowles & Hanson, 2018), this research suggests that good perception of privacy, authentication and risk management is achieved through:

- IT centers and training courses to help older adults in managing digital technologies.
- Including older adults in the process of designing new digital technologies.

Reference list

Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Two factor authentication using mobile phones. *2009 IEEE/ACS International Conference on Computer Systems and Applications*, 641-644.

Andrew, S., Watson, S., Oh, T., & Tigwell, G. W. (2020). A Review of Literature on Accessibility and Authentication Techniques. *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility* (pp. 1–4). Association for Computing Machinery, New York, NY, United States.

Becker, S. A. (2004). A Study of Web Usability for Older Adults Seeking Online Health Resources. *ACM Transactions on Computer-Human Interaction, Vol. 11, No. 4,*, 387-406.

Bell, C., Fausset, C., Farmer, S., Nguyen, J., Harley, L., & Fain, W. B. (2013). Examining social media use among older adults. *HT '13: 24th ACM Conference on Hypertext and Social Media* (pp. 158-163). Paris, France: Association for Computing Machinery, New York, NY, United States.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Minkyu, C. (2009). Biometric Authentication: A Review. *International Journal of u- and e- Service, Science and Technology, Volume 2*, 13-28.

Bowe, B. J., & Wohn, D. Y. (2015). Are There Generational Differences? Social Media Use and Perceived Shared Reality. *SMSociety '15: Proceedings of the 2015 International Conference on Social Media & Society*, 1-5.

Brewer, R. N., Schoenebeck, S., Lee, K., & Suryadevara, H. (2021). Challenging Passive Social Media Use: Older Adults as Caregivers Online. *Proceedings of the ACM on Human-Computer Interaction*, 123:1-20.

Brooke, J., & Jackson, D. (2020). Older people and COVID-19: Isolation, risk and ageism. *Journal of Clinical Nursing*, 2044-2046.

Cahn, A., Alfeld, S., Barford, P., & Muthukrishnan, S. (2016). An Empirical Study of Web Cookies. *Proceedings of the 25th International Conference on World Wide Web* (pp. 891–901). Montréal, Québec, Canada: International World Wide Web Conferences Steering Committee.

Carter, N., Li, C., Li, Q., Stevens, J. A., Novak, E., Qin, Z., & Yu, J. (2017). Graphical passwords for older computer users. *IEEE/ACM Symposium on Edge Computing* (pp. 1-7). San Jose, California: Association for Computing Machinery, New York, NY, United States.

Chiasson, S., Forget, A., Stobert, E., Oorschot, P. C., & Biddle, R. (2009). Multiple password interference in text passwords and click-based graphical passwords. *16th ACM Conference on*

Computer and Communications Security 2009 (pp. 500–511). Chicago : Association for Computing Machinery, New York, NY, United States.

Cristofaro, E. D., Du, H., Freudiger, J., & Norcie, G. (2013). A comparative usability study of two-factor authentication. *arXiv preprint arXiv:1309.5344*.

Currie, M., Philip, L. J., & Roberts, A. (2015). Attitudes towards the use and acceptance of eHealth technologies: a case study of older adults living with chronic pain and implications for rural healthcare. *BMC Health Services Research*, 162-174.

Department of Justice. (n.d.). *California Consumer Privacy Act (CCPA)*. Retrieved from Office of the Attorney General: https://oag.ca.gov/privacy/ccpa

Dworkin, S. L. (2012). Sample Size Policy for Qualitative Studies Using In-Depth Interviews. *Archives of Sexual Behavior, 41*, pages1319–1320.

Encyclopaedia Britannica. (n.d.). *Old age*. Retrieved from Encyclopedia Britannica: https://www.britannica.com/science/old-age

Flynn, K. E., Smith, M. A., & Freese, J. (2006). When Do Older Adults Turn to the Internet for Health Information? *Journal of General Internal Medicine, 21*, 1295-1301.

Frennert, S., & Östlund, B. (2016). What happens when seniors participate in new eHealth schemes? *Disability and Rehabilitation: Assistive Technology, 11:7*, 572-580.

Frik, A., Nurgalieva, L., Bernd, J., Lee, J. S., Schaub, F., & Egelman, S. (2019). Privacy and Security Threat Models and Mitigation Strategies of Older Adults. *Symposium on Usable Privacy and Security (SOUPS)*, 21-40.

Grimes, G. A., Hough, M. G., & Signorella, M. L. (2007). Email end users and spam: relations of gender and age group to attitudes and actions. *Computers in Human Behavior, 23:1*, 318-332.

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older Adults' Knowledge of Internet Hazards. *Educational Gerontology, 36:3*, 173-192.

Hope, A., Schwaba, T., & Piper, A. M. (2014). Understanding digital and material social communications for older adults. *CHI '14: CHI Conference on Human Factors in Computing Systems* (pp. 3903-3912). Toronto, Ontario, Canada : Association for Computing Machinery, New York, NY, United States.

Hu, X., & Sastry, N. (2019). Characterising Third Party Cookie Usage in the EU after GDPR. *Proceedings of the 10th ACM Conference on Web Science* (pp. 137–141). Boston, Massachusetts, USA: Association for Computing Machinery, New York, NY, United States.

Inglesant, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. *CHI Conference on Human Factors in Computing Systems* (pp. 383–392). Atlanta, Georgia, USA : Association for Computing Machinery, New York, NY, United States.

Knowles, B., & Hanson, V. L. (2018). The wisdom of older technology (non)users. *Commun. ACM 61, 3* , 72–77.

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., . . . Egelman, S. (2011). Of Passwords and People: Measuring the Effect of Password-Composition Policies. *CHI Conference on Human Factors in Computing Systems* (pp. 2595–2604). Vancouver, BC, Canada: Association for Computing Machinery, New York, NY, United States.

Lal, N. A., Prasad, S., & Farik, M. (2016). A Review Of Authentication Methods. *International Journal of Scientific & Technology Research, Volume 5*, 246-249.

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). *Social Media & Mobile Internet Use Among Teens and Young Adults.* Washington, D.C.: Pew Research Center.

Li, Z., He, W., Akhawe, D., & Song, D. (2014). The Emperor's New Password Manager: Security Analysis of Web-based Password Managers. *Proceedings of the 23rd USENIX Security Symposium* (pp. 465-479). San Diego, CA: USENIX Association.

Lian, J.-W., & Yen, D. C. (2014). Online shopping drivers and barriers for older adults: Age and gender differences. *Computers in Human Behavior 37*, 133-143.

Lüders, M., & Brandtzæg, P. B. (2017). '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, 19(2)*, 181–198.

Marky, K., Mayer, P., Gerber, N., & Zimmermann, V. (2018). Assistance in Daily Password Generation Tasks. *The 2018 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (pp. 786–793). Singapore: Association for Computing Machinery, New York, NY, United States.

Ministry of Social Development and Human Security. (2003). *The act on the Elderly, B.E. 2546 (2003 A.D.).* Bangkok: The Department of Older Persons, Ministry of Social Development and Human Security.

Nimrod, G. (2014). The benefits of and constraints to participation in seniors' online communities. *Leisure Studies Volume 33*, 247-266.

Norwegian Institute of Public Health. (2021, February 11). *Fakta om koronaviruset SARS-CoV-2 og sykdommen covid-19* . Retrieved from Folkehelseinstituttet: https://www.fhi.no/nettpub/coronavirus/fakta-og-kunnskap-om-covid-19/fakta-om-koronavirus-coronavirus-2019-ncov/

Nuchitprasitchai, S., Kilanurak, N., & Porrawatpreyakorn, N. (2020). Guidelines for Reducing Risk of Social Media Usage for Thai Elderly . *17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, 679-682.

Nyblom, P., Wangen, G., & Gkioulos, V. (2020). Risk Perceptions on Social Media Use in Norway. *Future Internet*.

Parida, V., Mostaghel, R., & Oghazi, P. (2016). Factors for Elderly Use of Social Media for Health-Related Activities. *Psychol. Mark., 33*, 1134-1141.

Politou, E., Alepis, E., & Patsakis. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity, Volume 4*, 1-20.

Quan-Haase, A., & Elueze, I. (2018). Revisiting the Privacy Paradox: Concerns and Protection Strategies in the Social Media Experiences of Older Adults. *SMSociety '18: International Conference on Social Media and Society* (pp. 150-159). Copenhagen, Denmark: Association for Computing Machinery, New York, NY, United States.

Renaud, K., & Angeli, A. D. (2009). Visual passwords: cure-all or snake-oil? *Communications of the ACM* , 135–140.

Rockmann, R., & Gewald, H. (2015). Elderly people in eHealth: who are they? *Procedia Computer Science 63*, 505-510.

Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P.-A., & Santos, I. (2019). Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. *ACM Asia Conference on Computer and Communications Security* (pp. 340–351). Auckland, New Zealand: Association for Computing Machinery, New York, NY, United States.

Schehl, B., Leukel, J., & Sugumaran, V. (2019). Understanding differentiated internet use in older adults: A study of informational, social, and instrumental online activities. *Computers in Human Behavior 97*, 222-230.

Schneier, B. (2005). Two-factor authentication: too little, too late. *Communications of the ACM, Volume 48*, 136.

Seifert, A. (2020). The Digital Exclusion of Older Adults during the COVID-19 Pandemic. *Journal of Gerontological Social Work, 63:6-7*, 674-676.

Shay, R., Komanduri, S., Durity, A. L., Huh, P., Mazurek, M. L., Segreti, S. M., . . . Cranor, L. F. (2016). Designing Password Policies for Strength and Usability. *ACM Transactions on Privacy and Security, Volume 18*, 13:1-34.

Shorten, A., & Smith, J. (2017). Mixed methods research: expanding the evidence base. *Evidence-Based Nursing, 20*, 74-75.

Sipior, J. C., Ward, B. T., & Mendoza, R. A. (2011). Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons. *Journal of Internet Commerce, Volume 10*, 1-16.

Soe, T. H., Nordberg, O. E., Guribye, F., & Slavkovik, M. (2020). Circumvention by design - dark patterns in cookie consent for online news outlets. *NordiCHI '20: Shaping Experiences, Shaping Society* (pp. 1-12). Tallinn, Estonia: Association for Computing Machinery, New York, NY, United States.

Statistics Norway. (1999). *Eldre i Norge, Statistiske Analyser 32.* Oslo: Statistisk sentralbyrå.

Statistics Norway. (2018, August 31). *Fire av fem nordmenn bruker sosiale medier*. Retrieved from Statistics Norway: https://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/fire-av-fem-nordmenn-bruker-sosiale-medier

Stephanidis, C., & Akoumianakis, D. (2001). Universal design: towards universal access in the information society. *Human Factors in Computing Systems* (pp. 499–500). Seattle: Association for Computing Machinery, New York, NY, United States.

Stobert, E., & Biddle, R. (2018). The Password Life Cycle. *ACM Transactions on Privacy and Security, 23*, 13:1-32.

Stokkenes, M., Ramachandra, R., & Busch, C. (2016). Biometric Authentication Protocols on Smartphones - An Overview. *Proceedings of the 9th International Conference on Security of Information and Networks* (pp. 136-140). Newark, NJ, USA: Association for Computing Machinery, New York, NY, United States.

Tennant, B., Stellefson, M., Dodd, V., Chaney, B., Chaney, D., Paige, S., & Alber, J. (2015). eHealth Literacy and Web 2.0 Health Information Seeking Behaviors Among Baby Boomers and Older Adults. *JOURNAL OF MEDICAL INTERNET RESEARCH*, 17(3):e70.

Topkara, U., Atallah, M. J., & Topkara, M. (2007). Passwords decay, words endure: secure and re-usable multiple password mnemonics. *The 2007 ACM Symposium on Applied Computing* (pp. 292–299). Seoul, Korea: Association for Computing Machinery, New York, NY, United States.

Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K., & Ben-David, S. (2012). Biometric authentication on a mobile device: a study of user effort, error and task disruption. *Proceedings of the 28th Annual Computer Security Applications Conference* (pp. 159–168). Orlando, Florida, USA: Association for Computing Machinery, New York, NY, United States.

United Nations. (2020). *World Population Ageing 2019.* New York: United Nations.

Walters, N. (2017). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? *AARP Public Policy Institute*.

WHO. (n.d.). *Older people & COVID-19* . Retrieved from World Health Organization: https://www.who.int/teams/social-determinants-of-health/demographic-change-and-healthy-ageing/covid-19

WHO. (2018, February 5). *Ageing and health*. Retrieved from World Health Organization: https://www.who.int/news-room/fact-sheets/detail/ageing-and-health

WHO. (n.d.). *Coronavirus*. Retrieved from World Health Organization: https://www.who.int/health-topics/coronavirus

Xie, B. (2011). Effects of an eHealth Literacy Intervention for Older Adults. *JOURNAL OF MEDICAL INTERNET RESEARCH*, 13(4):e90.

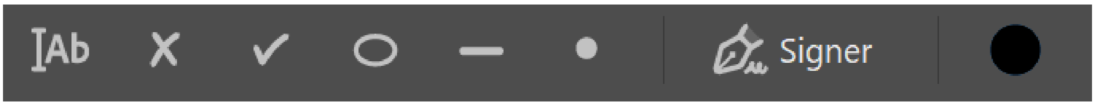
Appendices

Appendix A

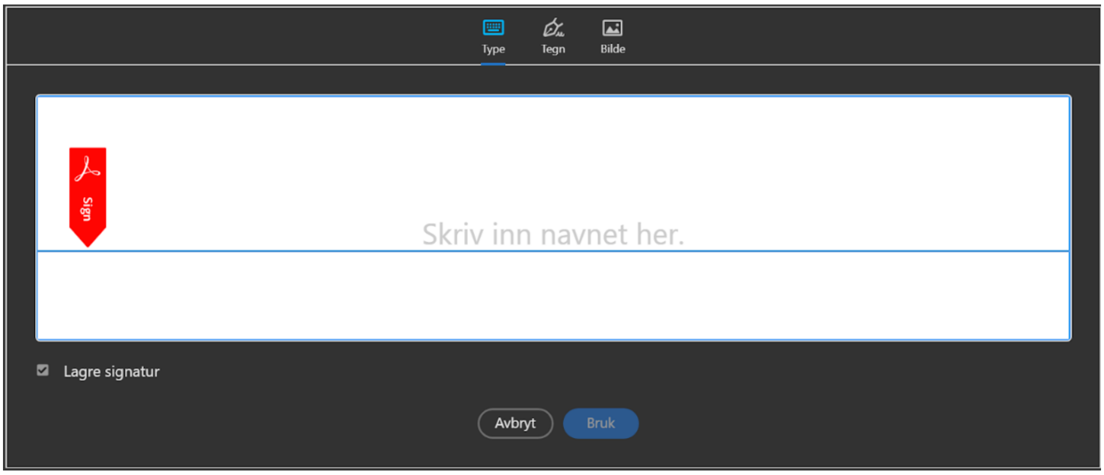
Signere PDF med Adobe

- Bruk Adobe Acrobat DC, og åpne PDF-dokumentet eller -skjemaet som du vil signere. Har du ikke Adobe Acrobat? Se «Installere Adobe Acrobat» på neste side.
- Klikk på signeringsikonet på verktøylinjen.

  Du kan også velge **Signer** > **Fyll ut og signer** i menylinjen øverst til venstre.
- Her får du en ny verktøylinje. Velg det første alternativet for å sette inn tekst (slik som dato), velg alternativene ✗ og ✓ for å krysse av bokser. Trykk på **Signer** for å signere.



- Velg **Legg til signatur**.
- Her får du tre alternativer:
  - **Type**, vil si at programmet genererer en signatur for deg, skriv inn navn eller inititialer.
  - **Tegn**, lar deg tegne en signatur med musepekeren.
  - **Bilde**, lar deg sette inn et bilde av en signatur du har lagret på maskinen.



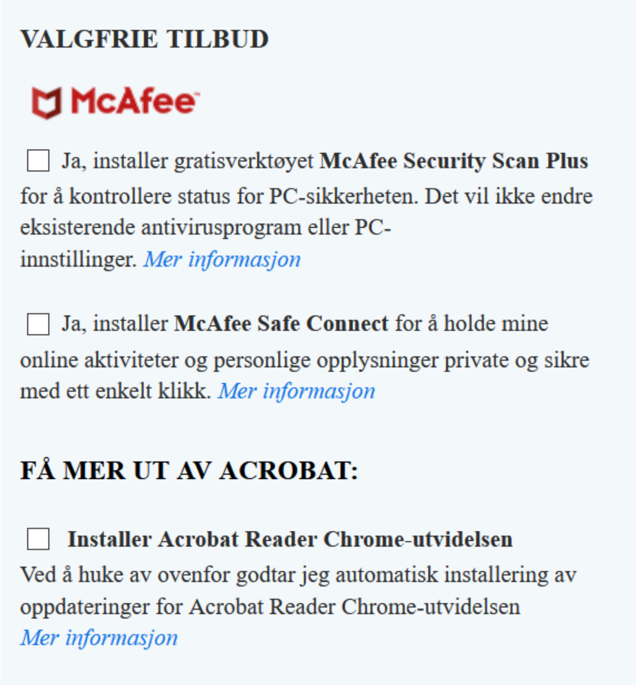
☑ Lagre signatur

- Velg hvor signaturen skal plasseres.
- Lagre dokumentet via **Fil > Lagre**, eller gi filen nytt navn og filplassering via **Fil > Lagre som…**

Installere Adobe Acrobat

Adobe Acrobat Reader DC er et godt verktøy for lesing og behandling av PDF filer. Programmet er gratis å laste ned og bruke. Det er tilgjengelig for de fleste plattformer, inkludert Windows, macOS, og Linux.

- Gå til https://get.adobe.com/no/reader/
- Jeg anbefaler å la feltene nedenfor stå åpne, ettersom du kan få programmer du ikke ønsker å ha på maskinen din.



VALGFRIE TILBUD

McAfee

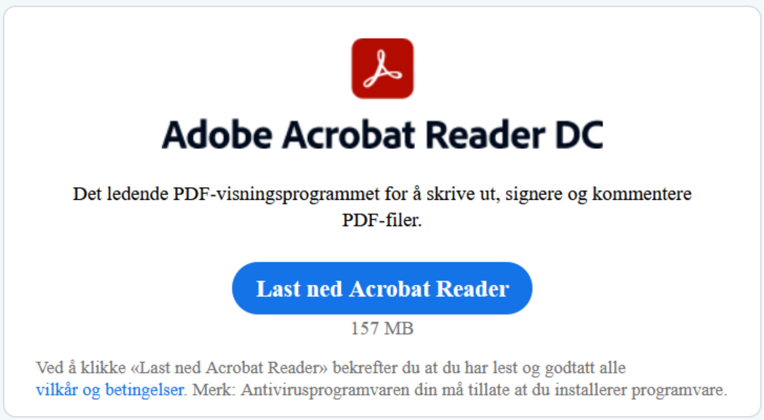
□ Ja, installer gratisverktøyet **McAfee Security Scan Plus** for å kontrollere status for PC-sikkerheten. Det vil ikke endre eksisterende antivirusprogram eller PC-innstillinger. *Mer informasjon*

□ Ja, installer **McAfee Safe Connect** for å holde mine online aktiviteter og personlige opplysninger private og sikre med ett enkelt klikk. *Mer informasjon*

FÅ MER UT AV ACROBAT:

□ **Installer Acrobat Reader Chrome-utvidelsen**
Ved å huke av ovenfor godtar jeg automatisk installering av oppdateringer for Acrobat Reader Chrome-utvidelsen
Mer informasjon

- Lengre ned på siden står meldingen **"Ditt system:"**. Dobbeltsjekk at det stemmer overens med ditt operativsystem.
- Deretter klikker du på **Last ned Acrobat Reader** og følger de videre instruksene systemet gir deg.



Adobe Acrobat Reader DC

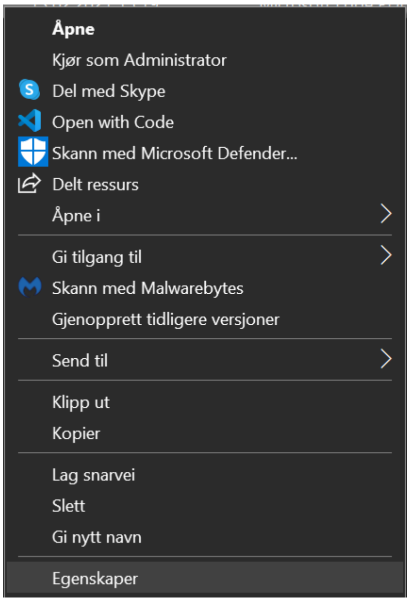
Det ledende PDF-visningsprogrammet for å skrive ut, signere og kommentere PDF-filer.

157 MB

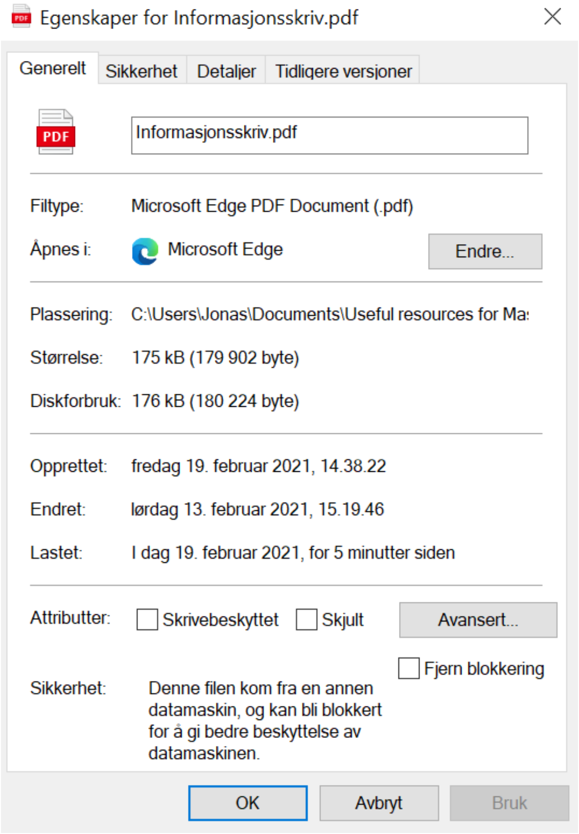
Ved å klikke «Last ned Acrobat Reader» bekrefter du at du har lest og godtatt alle vilkår og betingelser. Merk: Antivirusprogramvaren din må tillate at du installerer programvare.

Sett Adobe som standard program i Windows

- Høyreklikk på PDF filen, og velg **Egenskaper** nederst i menyen.



- I det nye vinduet står det “**Åpnes i:**”, her kan du trykke **Endre…** og velge alternativet for **Adobe Acrobat Reader DC**.
- Klikk deretter **Bruk** nederst i vinduet, etterfulgt av **OK**.



Egenskaper for Informasjonsskriv.pdf

Informasjonsskriv.pdf

Filtype: Microsoft Edge PDF Document (.pdf)

Åpnes i: Microsoft Edge

Plassering: C:\Users\Jonas\Documents\Useful resources for Ma:

Størrelse: 175 kB (179 902 byte)

Diskforbruk: 176 kB (180 224 byte)

Opprettet: fredag 19. februar 2021, 14.38.22

Endret: lørdag 13. februar 2021, 15.19.46

Lastet: I dag 19. februar 2021, for 5 minutter siden

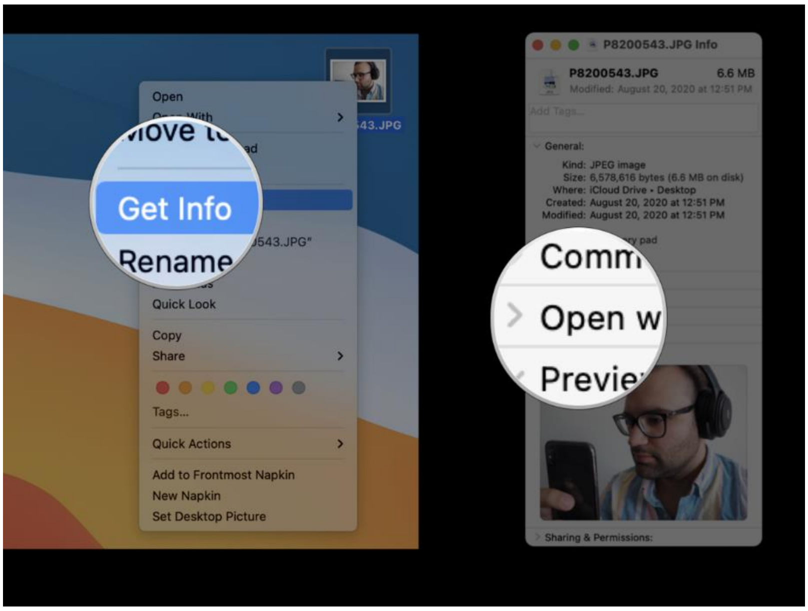
Attributter: □ Skrivebeskyttet □ Skjult

□ Fjern blokkering

Sikkerhet: Denne filen kom fra en annen datamaskin, og kan bli blokkert for å gi bedre beskyttelse av datamaskinen.

Sett Adobe som standard program på Mac

- Høyreklikk på filen, og velg **Info** i menyen. **Hint!** *Hurtigtast*: Klikk på filen én gang, og trykk **CMD** + **i** på tastaturet.
- Klikk deretter på fliken **Åpne med** hvis ikke den allerede er åpen.
- Deretter velger du **Adobe Acrobat Reader DC** fra nedtrekksmenyen.
- Velg så **Endre alle …** og så lukke vinduet med **OK**.



P8200543.JPG Info

P8200543.JPG 6.6 MB
Modified: August 20, 2020 at 12:51 PM

General:

Kind: JPEG image
Size: 6,578,616 bytes (6.6 MB on disk)
Where: iCloud Drive • Desktop
Created: August 20, 2020 at 12:51 PM
Modified: August 20, 2020 at 12:51 PM

Appendix B

PASSIVE STRATEGIES	DESCRIPTION	SUPPORTIVE QUOTES
BE CAUTIOUS AND SUSPICIOUS	Approach methods to identify malicious intent in mail, websites, and applications. It is important to keep a low profile.	"I believe, since I've been less active on social channels, and keeping a low profile, that I'm better protected than others" (P5). "I use 'language symptoms' on unfamiliar emails, people I don't know, who have noticeably bad language" (P12).
ACCEPT, IGNORE, AND IDENTIFY RISKS	Viewing information and using the internet "for free" often comes with a trade-off by sharing your personal data with other companies and data processors.	"I have a main idea that if we have this free access to the internet and all its benefits, you can count on that what we are doing is registered and "surveilled"" (P2).
SUFFICIENT BACKUP	Storing data on an additional storage media (e.g., cloud or USB) can be effective in restoring lost data in case of a breach.	"Sometimes I use a memory stick and transfer important files and documents et cetera. I would like to be better with backups, but I know how to use it, most files are on My Cloud" (P4). "I use Dropbox and OneDrive. I've scanned most of my own paperwork, so there's not much paper left" (P7).
USE FAMILIAR SERVICES WITH GOOD REPUTATION	Investigate a service before using it; ensure the reliance of the manufacturer; be confident that the	"There are cheap cloud services in China, but I don't want to store my data in China. I'd rather use those who are acknowledged" (P7).

	product is secure and does not cause any security threats.	“Before ordering something online, I tend to see how I can get in touch with the company. I also look for references and where they are located. I like to do a background check” (P16).
LIMIT OR AVOID THE USE OF DIGITAL TECHNOLOGIES	Restrictive use towards devices and online services; not engage in any online social events.	“I am more restrictive towards foreign websites. Very restrictive, I would say” (P20). “Personally, I think social media isn’t very good, particularly Facebook. They retrieve more data about me than what’s necessary, so I have limited my use of social media” (P22). “I do not want to manage finances on my phone, I have very few apps installed on it” (P23).
MASK FILES AND BROWSER HISTORY	Use anonymous names for confidential files; browse incognito.	“My system isn’t that advanced. I keep my passwords in an Excel-spreadsheet, but it is named something completely else. You wouldn’t recognize it amongst the hundreds of Excel-files that I have on my computer” (P12). “I have a list of all my passwords on OneDrive. It’s not named password, but something else, something anonymous” (P19).

ACTIVE STRATEGIES	DESCRIPTION	SUPPORTIVE QUOTES
USE PROTECTIVE SOFTWARE AND SERVICES	E.g., anti-malware, ad-blocker, and URL-scanner.	“On my machine, I have a security arrangement that you are probably familiar with. I use Norton. I feel like this program takes care of all the threats, ensuring the highest level of security for me” (P10). “From time to time, there are images and videos that are not showing up, which has to do with me using ad-block. Although troublesome at times, I prefer to have ads removed” (P14).
USE VARIED AUTHENTICATION METHODS	Relying on password managers and keychains, two-step verification, biometrics, and PINs.	“Remembering all those passwords is a problem. So, the more biometric methods, like fingerprints and such, the better” (P1). “Yes, I am using a password manager, Password Safe. It works great, I can synchronize it with my phone and everything. I’ve been using it for a while now, at least 10 years” (P3). “I am very happy using services that only require a fingerprint, and it’s fairly secure. Biometry combined with a password; it can’t get any more secure” (P16).
LIMIT USE OF DEBIT CARD ONLINE	Rather than using a debit card for online payment, use a credit card, or a service like PayPal	“I have a PayPal account, which I use from time to time. And I use Vipps and similar for payments” (P1).

	instead, which does not directly transfer between the bank accounts.	“I sometimes pay using Mastercard, but I don’t like it to be honest. Paying with Vipps feels way better to me. It makes me feel more secure” (P18).
CHANGE SETTINGS	Go through privacy settings, like location sharing; change preference for, and delete cookies; restrictive approach for social media sharing.	“I’m careful of sharing my location on the smartphone. It’s only the infection tracing app that I have allowed to share my location” (P12). “I look for privacy settings in the browser and Windows Defender, and for Malwarebytes of course” (P14). “I have been looking through privacy settings, but I should probably do it more often. It’s been a while since the last time I did it” (P23).
PHYSICAL SECURITY	Shut off devices which are not in use; keep security tokens and bypass cards behind physical locks.	“I have a habit of turning off my smartphone at night when I go to bed” (P15). “I use the chip for login, which I actually hide pretty well after each use. It’s never left out in the open, I tuck it into something and hide it” (P21).
REMOVAL OF UNWANTED MEDIA	Uninstall unnecessary software; delete mails from unknown senders	“If a mail pops up that don’t look familiar, I will just delete it. I don’t bother looking at them. This I’ve learned from myself” (P10). “I never click on foreign requests. If I see them in my inbox, I delete them right ahead” (P17).

MANAGEMENT OF PERSONAL INFORMATION	Personal information is only shared with integral services such as banks; refuse sharing personal information on social networking services.	“You know, one thing that I am sure of is to never share my social security number or account number to parties I do not trust. Also, if I share something, I always consider who I share it with” (P11). “I’ve been using Klarna for payments. They are asking me in a phone call about my name, date of birth and account number. Those three things. [Sarcastic] What else do you need? I do not want to share that” (P21).
DISCONTINUING SERVICES	Unsubscribe to services no longer being used; when a service or software is too complex, abandon it rather than wasting time.	“I’ve seen a problem faced by many adults. They tend to pay too much on services they do not use, because they lack knowledge. I once helped a lady who monthly paid for two internet bills. Completely unnecessary! On top of that, their mailbox tends to get flooded with spam, and they do not know how to unsubscribe. Often, it’s hidden at the bottom in a very small text” (P16).