Protecting Older Adults Online

A personalised approach of presenting account security protections to older adults

Melvin Abraham
University of Dundee
Dundee, UK
mabraham@dundee.ac.uk

ABSTRACT

Older adults are classed as the most vulnerable generation [3, 6] to cybercrime such as digital identity fraud or financial loss [33] due to a stereotyped general lack of technological knowledge and understanding of security best practices. However in today's age older adults are increasingly becoming more technologically proficient, using the internet more and increasing their technical literacy. Even with the advancements, older adults are still victims of unusable security practices and practices that are not fit for purpose when considering the older adult's needs. Thus creating the need for older adults to alter recommendations and practices to work for them. Potentially creating a divergence when comparing what risk actually exist and what risks are perceived to exist, leading to a false sense of security.

This project investigated the mindset of an older adult regarding account security, their perceptions of the cyber risks they face and investigated what the typical account structure created by older adults looks like. A web application was created to analyse and identify the reality of security vulnerabilities present within the older adults account structure which was used to compare both reality and perception of the risks present. Later the analysis was visualised to provide tailored security advice, aiming to empower and improve the resilience of older adults towards cyber-security attacks.

1 INTRODUCTION

Older adults (70+) are an underrepresented demographic when it comes to using web systems, and can unconsciously be ignored when designing secure systems [52]. An increasing number of older adults are using the internet [53], smart devices (IoT) [4, 17] and increasing their technological literacy though initiatives such as Age UK's IT Training [50] and university level programmes (e.g. Dundee User Centre [9]). However, older adults are still seen as the most vulnerable generation to online cyber attacks [3, 6] due to a general lack of knowledge of online security risks [7, 12, 20]. In the United States just under $40 billion is stolen from older adults on average by cybercriminals [33]. This number could be considered as a low estimate as older adults are usually unwilling to report such crimes due to fear of embarrassment [29].

A little understood challenge that is faced when adopting online security practices is related to authentication methods and how these are shared between accounts. It is possible for accounts to be accessed using more than just the primary authentication method [23]. Seeing the links between accounts and physically real world attributes is a way of seeing issues you may not have noticed [23]. For example, if a password for an email address is leaked then every account which is linked to the email is also leaked transitively through a potentially reused password or by an accounts recovery method.

It has been suggested that on average people own 16-26 active online accounts [15, 40, 41, 55]. Companies offering password management services claim that their users today have an average of 70 (NordPass [39]), 150 (Dashlane [8]), or even 190 (LastPass [47]) online accounts. While these numbers must be taken with a grain of salt, even the most conservative of these claims, is vastly larger than the number of complex passwords that a typical human can memorise let alone an older person [54]. The sheer number of accounts a person needs to manage will inevitably lead to adopting poor security practices, such as reusing passwords [54].

To this end, this project conducted semi-structured interviews with 7 older adults (70+). In each of the 90 minutes interviews the participants were asked questions in order to understand their mindset regarding online security, their current practices and investigate what connections exist between their online accounts are as well as how they connect to real world items and devices. The results of the interviews were then interpreted into created personas, requirements and prototype designs with regards to prior work within how older adults use technology and guidelines of usable security. Ultimately leading to the creation of a novel visualisation of account structure information, in order to provide personalised and usable security advice to older adults. Finally, potential future work is presented that could contribute to advancements in this area.

1.1 Work Contributions

This project makes two contributions:

(1) A dataset of Account Access Graphs relating specifically to older adults. This includes an examination of patterns and commonalities that exist within account ecosystems created by this group.
(2) A method to visualise an account ecosystem. This visualisation highlights well protected areas within the ecosystem that do not need any further modifications along with vulnerable points that are at risk of potential attack. These visualisations allow for a novel analysis to identify and classify vulnerabilities within account access data found in a personal account ecosystems.

2 RELATED WORK

2.1 Cybersecurity Risks for Older Adults

Older adults are particularly at risk to attacks aimed at their online security when compared to other age demographics. In general, older adults tend to have a significant sum of retirement savings

and it comes as no surprise that this demographic is targeted more often than others for internet crime and fraud [35]. In society older adults tend to be more isolated socially [2] and can lack experience when it comes to digital literacy with this including use of the internet [37]. These factors together are critical, as research shows people who have weak ties with society, combined with low digital literacy often cannot take part in the learning that occurs within social networks [38]. These factors leads to people becoming more trusting and vulnerable to fraud and social engineering attacks [2, 20, 21]. The impact of these attacks are amplified for this group as older adults also have less in place to protect themselves against spam and phishing attacks compared to younger adults [21].

Older adults tend to be more likely to fall victim to a specific set of scams disproportionate to those in other demographics. A contributing factor is that older adults require more time to read information online before they are able to make a judgement on its reliability [24]. Being overly trusting and taking information at face value causes the user to lack the means to gauge the accuracy of the advice they receive [49]. Older adults have a low risk threshold regarding technology and are likely to follow advice given [31] with this potentially also being true when the advice is malicious in intent. This leads to a chance of accepting and believing fake news [32], an increased risk of social engineering [32], and a potential false sense of security by entrusting others such as family members [27, 42] with their security choices which should never be considered an appropriate security strategy [16, 17].

2.2 Accounts and Passwords

Passwords are commonly viewed as the best method of ensuring account security online, due to their simplicity and cost effectiveness [25]. People commonly use this method to secure their online accounts and it is estimated that an individual owns 16-26 active password protected online accounts [15, 40, 41, 55]. Even the most conservative of estimates for accounts an average person has is still a lot for one person maintain securely let alone an older adult.

The National Institute of Standards and Technology (NIST) cybersecuirty framework provides password guidelines and policy which aims allow users to create stronger passwords (NIST SP 800-63 [19]). Examples from the guidelines are that a password should be at minimum 8 characters or longer if created by a human [19] and that priority should be given to password length over complexity. This advice contradicts traditional password policies to create complexity such as at least one uppercase, one lowercase, a number and a symbol [19] and NIST reported that overly complex passwords can lead to poor password etiquette as users tend to forget the original complex password and replace it with a weaker one [19].

Password reuse is a common method used by people when securing their online accounts [54]. Password reuse occurs when a single password is used to access more than one accounts [10] and is likely due to challenges that are faced by people when attempting to remember multiple complex pieces of information [54]. Password reuse creates an account security vulnerability which an attacker can exploit [10]. When one shared password is discovered for a user through methods such as a password database breach [10, 25], dictionary attack [25] or just guessing, every account that shares the same password is also compromised [25, 28].

One method that can be used to remove password reuse is for users to rely on software such as password managers. Password Managers are essential tools, created to prevent two problems: the use of weak passwords [41] and the reuse of passwords [34, 41]. The password manager industry itself is growing, by 2025 the whole world-wide industry is expected to be worth more than $2 Billion dollars [51].

Despite the clear benefits in this technology, adoption rates for password managers with built in password generation features are poor [41, 48]. Adoption is even lower for older adults with suggested reasons for this being a lack of independence, trust and usability [43]. Non-users of password managers claim they ‘do not have a need for one’ or are more suspicious of all their accounts are stored in one place [14, 41]. The latter point brought up by non password manager users does hold some merit, the master password to access the password vault must be secure and unique or a false sense of security is created [41] with the same vulnerabilities mentioned when reusing a password [25, 28].

It is important, however, to consider that password managers themselves come with issues in their implementation. Password managers can only focus on individual accounts and ignore how accounts link with each other. A look at the bigger picture outside the blinders of individual accounts brings to light critical security issues and lack of best practices [23] which cannot be identified when accounts are considered individually [23].

2.3 Account Access Methods

Many methods can be used to access an online account outside of the primary authentication method [23]. This can include options such as account recovery or a single sign-on such as ‘Sign In With Google’ [18]. People rely on this combination of different digital systems and real world artefacts as a way to add perceived security to their accounts.

With each system and artefact that is added into the security practice of an individual, their account access graph (i.e. a representation of how accounts and artefacts link together) grows. This growth can occur due to links between an online account and a physical object when the authentication method requires both entities to securely gain access to a system. Examples of this include a password and a phone used for two-factor authentication [23] or if a password is written down in a diary.

2.3.1 Account Access Graphs. An Account Access Graph is a directed graph to used to model how accounts link together. Nodes within the graphs resemble accounts, devices, sensitive information or physical objects. While the edges resemble the methods available to access the node the edges are directed towards.

The links between items on an account access graph are not limited to 1:1 relationships between items. 1:m, m:m, and recursive relationships can also occur. This can happen due to situations where an email is used to login to a social media account, a password is reused between the accounts, or a password manager is used to assist in keeping password unique [23].

Coloured edges resemble logical AND/OR operators as seen within decision trees used by expert systems. All the edges of same

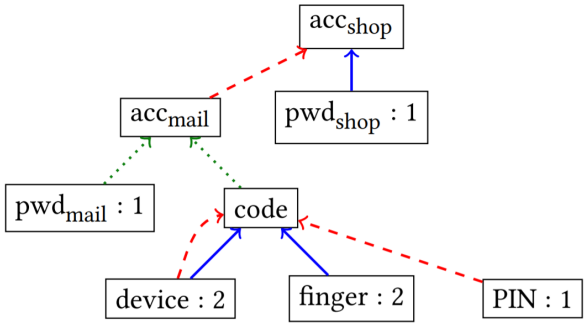

Figure 1: Example of an Account Access Graph from Hammann et all [23]

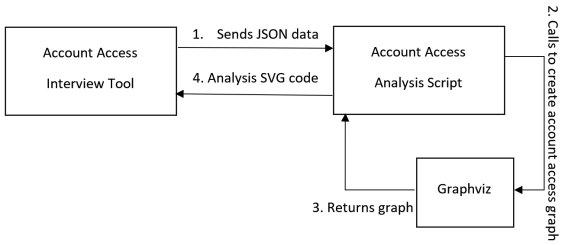

Figure 2: Flow of data when analysing account access information using the Account Access Interview Tool

colour when directed to a node create a logical AND link as all the edges are required to form an individual access method.

Edges where the line is dashed resemble recovery methods to access the account. For example when clicking 'Forgotten my password' and a recovery email is sent to a designated email address.

As seen in Figure 1 the shop account which is modeled by node acc_{shop} can be access using two methods 1) supplying the correct password (pwd_{shop}) or 2) accessing acc_{shop} through the nodes recovery method acc_{mail}.

An account access graph allows for security vulnerabilities to be identified that may not have been visible when examining accounts in isolation of each other. Such as, a user may implement two-factor authentication for all their social media accounts using an authenicator app on their phone, thus feeling a sense of security. Yet, if the pincode protecting the app from unauthorised access and the pincode to unlock the phone are the same, then an attacker only requires access to the phone in order to compromise all of the accounts which are accessed through the authenticator app.

Currently, the creation of an account access graph requires interacting with a security expert who can analyse the graph and suggest modifications. Links within an account access graph create a chain, which can be dangerous. As the accounts linked within the chain are only as secure as the weakest entity in the chain, when one item is compromised by an attacker all the other accounts connected within chain will be compromised too [23].

2.3.2 Account Access Graph Creation Tools. An Account Access Interview tool was created by the author as part of a research internship programme (See Appendix H). This tool allows the interviewer to systematically ask specific questions to track accounts and devices. Thus allowing the interviewer to map how each entity is accessed and how links are formed within the participants personal account ecosystems.

This tool collects information to see the big picture of what the participants account access graph look like. This information is currently exported into a JSON file which is then optionally fed into a graph analysis script built by Dr Saša Radomirović and then rendered using Graphviz. This analysis helps advise the security expert on critical points within the graph they might want to take a closer look at when providing comments to the participant (data flow is explained in figure 2.

There is still yet to exist a system that can automatically provide account security advice to a user **without** the need of a security expert present, let alone personalised and appropriate advice for the specific issues older adults face compared to a more general demographic.

2.4 Communicating Security Specific Issues and Recommendations

When designing effective methods to communicate warnings and alerts to grab a users attention of an issue or urge them away from danger, fundamental guidelines and standard can be found. Communicating safety critical information in a digital medium with regards to user experience has been researched in depth in the field of Usable Security such as the readability of the message [5] and interaction elements of the message [11].

When creating phishing warnings, research finds that warnings alerts or messages should be clearly distinguishable by severity levels [13] for example '*High*', '*Medium*' and '*Low*' thus making important information clear to the user, paired with showing the user the information upfront and not within in a "*learn more*" section, as these links are rarely ever viewed [1]

Security information should be clear to the user and in their own words [26, 44]. When recommendations are communicated using their words the user understands and is personal, users tend to feel more attached to the message and feel that the recommendations are in their own best interest [44].

Using bullet points is an effective means of communicating to the user the risks of their actions as it is easily understandable [45, 56]. It is found that the majority of users hesitate when it comes to setting up new a security practices such as Two-Factor Authentication due to not understanding what the practice is, what they are required to do up front and importantly what it means for them. [44].

2.5 Research Questions

Older adults as a demographic are regularly victims of cyber crime, as older adults tend to be seen as less technologically literate. In order to protect older adults from these attacks, it is first important to understand how older adults approach security, and what accounts they have in order to understand how they can be protected.

In order to create a high standard of account security, the individual must have an understanding of their accounts and the possible vulnerabilities present. Due to older adults lacking experience when it comes to digital literacy, their perceptions and bias mean that their current level of online security may not be accurate, thus creating vulnerable points within their personal account ecosystems.

From the information above, the following research questions must be answered:

RQ1- What do personal account ecosystems created by older adults look like?

RQ2- What differences exist between older adults' perceived awareness of account security and current security vulnerabilities?

3 OLDER ADULT ACCOUNT ECOSYSTEMS

In order to understand what the typical personal account ecosystems of an older-adult look like, 7 Semi-structured interviews were conducted in January 2021 each lasting between 60-90 minutes over video conferencing software in order to protect the safety of both the interviewer and participants in light of the Covid-19 pandemic.

Each interview was conducted by the same person to ensure coherence and consistency between all the interviews. Before hand 4 pilot interviews with peers took place in order to gauge length and flow of the interview. The answers and modeled Account Access Graphs from the pilot interviews are not included in the results of this user study.

The semi-structured interviews had two aims. The first aim was to understand the what individual's personal perceptions were of security risk, vulnerabilities and best practices and if they had or lack of the mentioned issues in their own personal account ecosystems.

The second aim was to answer research question 1 directly, to investigate what the older adults personal account ecosystems looked like in regards to how accounts, devices, information and physical items connect with each other. The older adults personal account ecosystem was modeled as an Account Access Graph [23] as seen in the Section 2.3.1. Using the Account Access Graph model, account vulnerabilities and lack of account security best practices were found.

3.1 Materials and Equipment

Demographic Information: Participants were recruited from North East Scotland, through the help of the University of Dundee's User Centre. From our 7 participants 5 were female and 2 were male. The ages ranged from 70-90 years old (mean=75.4). All participants are retired and none were from an IT or related field. All 7 participants stated they have a reasonable competency when using technology for day to day tasks such as communication, information retrieval and online shopping. 3 participants previously worked in the medical sector, 2 in educational teaching/advising, and 1 in economic development. All participants consented that their responses could be quoted and used, we refer the participants of this study as P1, ...,P7.

Account Access Graph Data Collection: To gather the account access information in order to create the participants Account Access Graph was conducted using the Account Access Interview Tool described in Section 2.3.2. This step can also be replicated manually using the interview script in appendix G.10 as a backup option if need be however this was not used during the study.

Interview Setup: The semi-structured interview took place using the Zoom Video conferencing software [57]. When the account access graph was being created the interviewer's screen was shared with the participant to allow them to see the account access interview tool, this was done to aid the participants memory and lower mental strain that could be caused from remembering the answers they gave though out the process.

***Interview Script*:** An interview script was used to maintain a high level of consistency and coherence between all of the interviews. The script was designed specifically to follow a semi-structured approach allowing for conversations to flow naturally were any interesting points brought up could be explored and elaborated.

Experimental Procedure: Before each interview the participant was sent an information sheet and digital consent form containing information about the project. Interview topics were split into two parts 1) discussion of account security based on the participants experiences and views and 2) creating the participants Account Access Graph. The interview script for part 1 is shown in appendix F.3

The interview started by asking questions to gauge demographic information. After this was completed the *Account Access Interview Tool* was used to gather information relating to the individual account setups of individual participants. Participants were systematically asked what accounts or items they have under specific categories: Devices, Password Managers, Emails, Social Media, Finance, Shopping, Entertainment, Gaming, Other and a summary of all the passwords. Participants did not declare every account they have ever created as it would be impractical due to the number of *'one off'* accounts a person creates but were urged to mention accounts that were important to them in each category, or that store sensitive information such as banking details.

In order to protect the privacy of the participant, each item and account was given a nickname assigned by the participant, in order to communicate sensitive information such as a password or an account name. For example a nickname for the participants password that is used to access their email could be *'EmailPassword'* or *'password1'*. Participants were given the opportunity to revisit answers they had previously provided in order to review the nickname and the access methods.

Once the all the account access information was collected to form an account access graph, the participant was asked questions relating to how they go about finding information security advice, with this following the studies *Interview Script*. Participants were asked questions to elaborate on their day to day online security, specifically regarding their views, practices and strategies that were formulated from their lifestyles and experience with online security.

The interview was concluded by asking the participant if they was anything they wanted to bring anything up that they felt was missed during the interview, that would be beneficial for this study. The topic would be discussed if the participant had any insight they wished to share, followed by a short debrief at the end.

3.2 Results

All interview sessions were analysed by the author. Every attempt was made to keep the interviews impartial however, a potential avenue where bias may be present is that the author was present when each interview session was conducted. A structured interview guide was used to reduce this risk.

The interviews were transcribed, anonymised, and annotated by the author before analysis. Sections of the interviews from all the participants were combined and were inspected individually based on components of the interview guide. Conclusions found within the results are formulated from the trends seen within the data and notable features are also highlighted.

3.2.1 Security practices used by older adults. Older adults use a number of security practices to keep themselves secure online. Participants discussed their usage of passwords, password management systems, and a suspicion that is present when using online services.

Passwords: From the participants that were interviewed all of them indicated that they follow basic account security hygiene, they stated they do not reuse passwords "*every password for every account is unique*" (P1) as, "*the domino effects to all your other accounts when one password gets compromised is clear*" (P7). P2 described their password creation strategy as "*taking a password and changing it around, so that every password is a little different and not the same as another one that I have*".

Password Management: Memory was a critical factor to all of the participants, using memory alone to remember passwords was not a fit for purpose solution. Their password management strategies were paramount in the participants independence to use their online accounts. Only one participant (P3) stated they use a paid digital password manager the rest of the participants stated they used unencrypted password management methods such as "*writing passwords down in an address book*" (P4), or "*store my passwords in a word document*" (P2).

> P7: "*Using a password to unlock my phone is not something I can do, when you are my age you tend to find yourself forgetting things quite often ... however I can't write the password down for the same reason, if I ever forget to take my book with me, then I wouldn't be able to use my phone*"

Online Suspicion: All the participants also stated they are very careful when it comes to being online, as they are "*very suspicious*" (P1) when it comes to clicking on any links online when browsing or "*links within emails in case it's spam*" (P3). Out of the 7 participants, P2 and P6 stated they go out of their way to maintain their online security "*by using Apple products as they have more protections out of the box*" (P2) and "*clearing the browser cache to remove any cookies*" (P6) in order to add another layer of security.

Every participant mentioned their reason for their efforts stems from an urge to feel a sense of security, "*If an attacker found one issue they would feel motivated to find more*" (P7) . Being highly aware that adults of their age are regularly victims of fraud and cyber attacks, a fear 75% of the participants share was "*becoming another target*" (P3).

3.2.2 Mindset of the older adults regarding online security. The mindset of being secure online is something all the older adults share. Participants discussed the different mindsets they have established through their experiences of trying to be safe online.

Attitudes towards security: Each of the participants hold the belief that it is "*very important*" (P4) to be secure online, especially when it comes to "*accounts that handle financial transactions*" (P5) such as banks and "*online shopping websites*" (P5). All the participants stated that their motivations and mindset stemmed from fear of "becoming a victim" (P1) of cyber crime that and undertaking "*a financial loss*" (P5). P3 even brought up the view that "*hackers are a lot smarter than me ... they will find new ways to scam people*", thus P3 finds "*it's our own responsibility*" to stay secure and up to date with the current best practices.

Perceptions of security: All the participants feel that "*they are reasonably secure*" (P1) when it comes to their account security and being online. Each participant stated they are "*doing the best I possibly can within my ability*" (P7). All the participants stated they have "*never previously been a victim*" (P4) of an attack which leads to creating a sense of validation that "*I must be doing something right*" (P1) as their efforts are effective and "*don't need to worry just yet*" (P5) about their online security at the moment. An interesting view that was brought up by two participants (P2 and P3) were that third parties also play a role in insuring their online safety, in P3's case it came down to "*doing research to see if you can trust a company to keep their systems secure for example my bank*" and P2 stated that "*my children will pull me up if I am doing anything I shouldn't be*" and act as a safety net to mitigate actions that may lead to being a victim of fraud or an attack.

3.2.3 Factors that contribute when deciding which security practices to implement. An older adults has many factors to consider when researching if a security practice is suitable for them. Participants discussed the roles of trust, understanding and usability play when deciding to impalement a practice.

Trust and Understanding: Both these factors play a fundamental role to the participants when deciding which practices to implement. A common theme seen between all the participants was that they will not implement a security practice without "*dedicating a good amount of time into researching the topic to understand*" (P6) the practice. As mentioned before the participants tend to be more conscious when it comes to being online and will only perform tasks that they "*understood fully and trust nothing will go wrong*" (P4). Not only are the practices required to be trusted but also "*must be recommended from somewhere that is respectable*" (P3) and reputable. P1, P2 and P4 also indicted that "*recommendations from a trusted friend*" (P2) can also substitute for their own thorough research into the practice.

Usability: All the participants bar one stated that they have faced "*difficulties*" (P4) due to the lack of usability considerations which have lead participant to "*spend to extra time and effort*" (P6). Usability of the security practice is the principal factor when it comes to deciding which security practices will be implemented and which will be discarded. P5 shared the view that "*life is too short to spend more time than you need to*" similarly P6 expressed if they are going to implement a security practice, "*the extent of the reward* (how much more secure they will be after the implementation

compared to before implementation of the practice) *must justify the effort required to do so*".

3.2.4 Effective means to communicate information security advice. When older adults are researching information security advice the means of communicating that information play a key part. Participants went on to explain the effectiveness of textual advice and information presented through a walk through format.

Text Based: 5 out of the 7 participants (P1, P2, P4, P6 and P7) stated that if the information is in a written format such as an "*an article would be ideal*" (P1) as it "*allows me to spend time to analyse and go over the advice*" (P6). However a view point that was mentioned by P3 went against the idea of a long articles but in fact that if something was important "*give me a short and concise message on what to do*". P3 also mentioned that they found it difficult finding information that can be acted on quickly as "*the information is out there but it is not easy to see only what you need to do without the fear of death being thrown at you*" referring to some articles being written to have a heavy emphasis on what will go wrong if the practice is not implemented than the actual practice itself.

Walk-through: Out of the 7 participants, 4 (P4, P5, P6 and P7) indicated that relying on a trusted source to inform them on the topic they were researching such as a "*trusted friend*" (P4) "*there to walk me though it*" (P7) , "*a video*" (P6) or a "course on security" (P7) were effective means to communicate information.

Though it is important to note that the main selling point for communicating advice using a walk-through format was the ability to "ask questions and have a conversation" (P7). P4 mentioned that if there was someone explaining concepts "*they would have the chance to get information that answers my exact question*", thus getting access to personalised advice than broad general information where one size fits all.

3.2.5 Account Access Graphs representing account ecosystems made by older adults. When the 7 account ecosystems created by older adults are converting into account access graphs (see example of P2's account access graph at figure 3), quickly patterns and consistencies become more prominent such as password hygiene and which current best practices tend to be present and which do not.

When analysing the graphs it shows that **the participants have between 16 and 53 nodes with an average of 33 nodes**. Also present, are a wide range of edges from a minimum of 36 up to 113, **with an average of 59 edges**.

It was found that from the nodes present in the graphs **between 6-22 were accounts** thus the older adults had **12 active accounts on average**.

However, as described in the *Experimental Procedure*, the participants were only required to declare the main accounts they have actively use or accounts that store sensitive information.

When identifying **the most connected nodes within the graph it was found that the participants primary email address** were the hub nodes a trend see in all the the 7 account access graphs. The email address was used to create all the accounts within each graph moreover **each account could be directly accessed using the email alone as as recovery method**.

It is clear that each of the participants have incorporated password management strategy into their graphs. The strategies can be classified in 3 ways, solely non digital methods as seen in the graphs of P1, P4, P5 and P7, digital methods which was only seen in the graph of P3 or a combination of both digital and non digital methods as seen the in the graphs of P2 and P6.

Through the use of a password management technique the **number of reused passwords are low** for example in the graph of P1 and P7 0 passwords are reused to access more than one account or P5's graph where only 1 password out of 8 were reused.

The adoption rate of multi-factor authentication being used throughout the graphs were low. A trend is clear and present in all the older adults graphs are that the **older adults only enable multi-factor authentication to accounts that require the practice by default** such as financial accounts.

The final feature that was present in almost all the account access graphs were the **older adults common usage of authentication methods enabled to unlock their devices**. Each device could be unlocked using either a password, pincode or using a biometric authentication method such as fingerprint scanner or FaceID. It was noted that in the graphs of P4 and P7 none of the devices used authentication methods.

The full dataset of the account access graphs and their corresponding JSON files can be viewed in appendix K

4 A SYSTEM TO ENGAGE OLDER ADULTS IN ACCOUNT SECURITY

In order to enable older adults to develop an understanding of the security vulnerabilities that exist in their account infrastructure, a system was created that provides a personalised account security analysis. The following broad design requirements have been established based on previous literature, results from the semi-structured interviews that were conducted, and an analysis of the account access graphs which were created by the older adults:

(1) **Analyse Account Structure:** The analysis should identify critical security vulnerabilities and missing best practices within an older adults account structure information.
(2) **Clear Information:** The results of the analysis should be presented in a format that is clear and usable enough that an older adult can understand and implement the advice in a way that works for them.
(3) **Appropriate Advice:** The system should provide recommendations and solutions for each security issues found.
(4) **Quantify Security:** This system should be able to quantify an individuals security in order to give context in how to become more secure.

This system is a dynamic web application built using React [46] and Flask [22]. When the older adult uploads their account structure information they created during their account access interview, the information is converted into an account access graph where a collection of tests and analysis' are conducted in order to find security vulnerabilities.

See full webapp here: https://protecting-older-adults-online.herokuapp.com/#/

More information can be seen in the appendix for information regarding requirements in the form of user stories (B.1), system design, development, professional, legal, ethical and social issues.

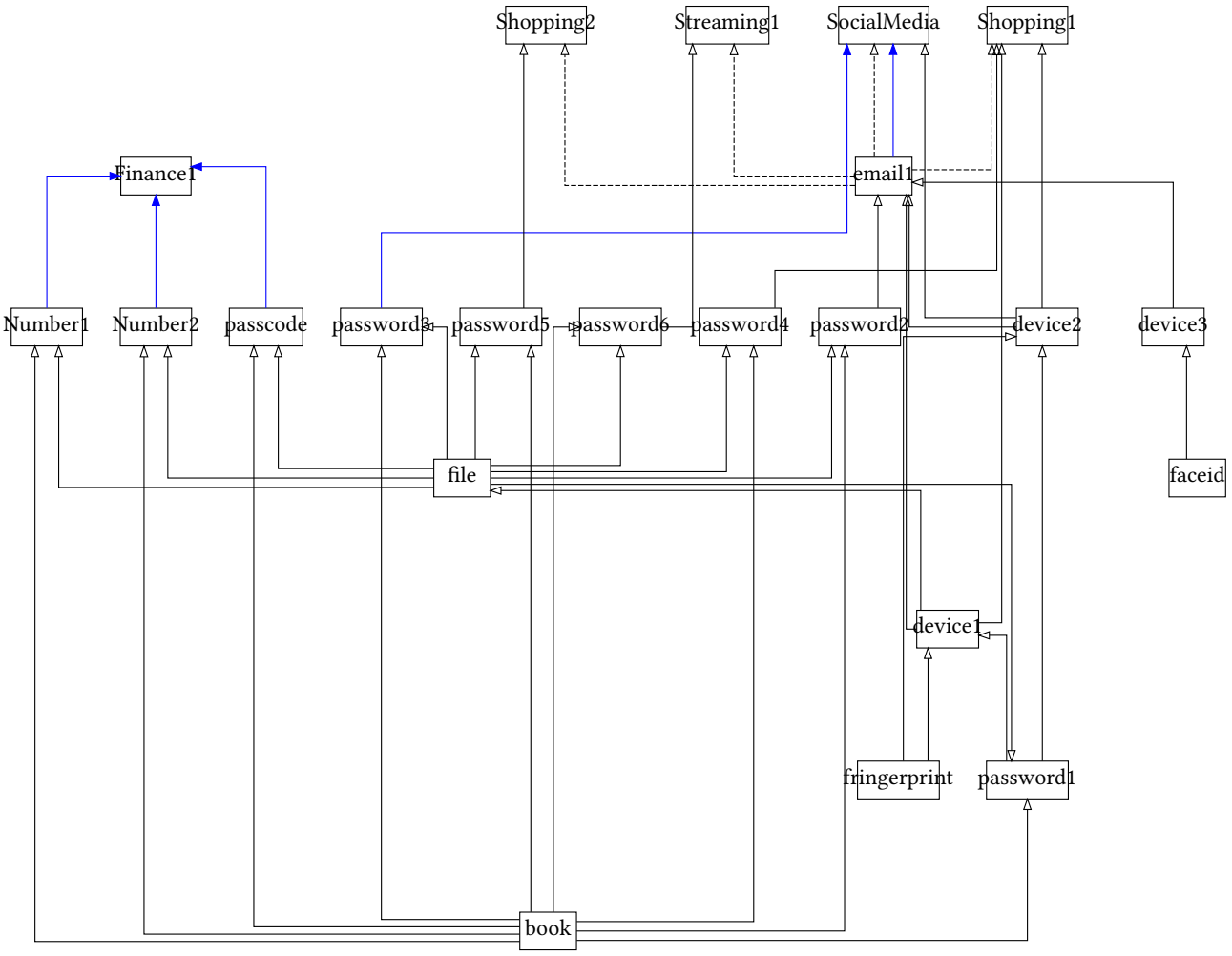

Figure 3: P2's Account Access Graph

4.1 Analysis of the Account Access Graphs

To analyse the account access information, the account access graphs where fed into several tests, each aiming to achieve one or more of the following objectives. To find '*Critical Issues*'- these were vulnerabilities that created major problems compromising the older adults account security which should be fixed as soon as possible. Secondly to find vulnerabilities which are preventing the user from '*Achieving Best Practices*'- this is usually caused by not staying up to date and implementing current standards and best practices, these results ideally should be given attention after the all the critical issues are fixed if any are present. Finally the last objective is to find '*What the use is doing well*'- in order to validate their efforts and bringing to their attention practices the user may not have been aware of that are protecting them. Showing information like this can potential go a long way in motivating the user to take on the recommendations found though the analysis, giving them a feeling of self belief that they are capable of being secure.

4.1.1 Critical Issues. There are 3 main types of vulnerabilities which can be searched for within the account access information, issues regrading authentication methods, weak passwords strengths and comparable devices.

To find a password that is being used to access multiple accounts- a reused password within the graph, first find which nodes within the graph represents a password and for each password node count at how many edges are directed away from the original password node, if the number is greater than **one** then the password can be classed as reused.

Devices that do not use any authentication methods to unlock can be found by traversing the account access graph to identify all the nodes that represent a device, for each of the nodes check how many edges are directed towards the device and count how many of those edges come from nodes representing a Password, Pincode, or Biometric authentication method such as Facial or Fingerprint scanning.

Passwords that are weak in strength can be found by traversing the graph to find the nodes which are passwords, and checking the

strength assigned by the user during the account access interview. A strong password- a password that was created automatically from a password generator and importantly **not** created by the user. An average password- a password that **was** created by the user, that they class as secure. Finally a weak password- a password that **was** created by the user, that they class as not secure or a password that does not fit in the other two categories.

4.1.2 Achieving Best Practices. Finding the most important node within the account access graph can be accomplished by identifying the graphs hub nodes, which can be found by traversing the nodes within the graph to find which node have the highest number of edges directed away from the node.

Finding the passwords where the strength may not be up to standard can be performed the same as finding weak passwords as mentioned above, traverse the nodes which are passwords and check the strength to see if the user stated this password was average in strength during the account access interview.

Checking if the user uses a Password Manager to store their passwords can be found using one of two methods:

(1) Traverse the graphs and identify if any nodes are of the type 'Password Manager'.
(2) Go directly to the nodes which as passwords can check the inward edges coming into the node to see if any of the edges originate from a node with the type 'Password Manager'.

Both method 1 and 2 have a time complexity of O(N) where N is the number of nodes being checked but usually based on the implementation of the graph method 2 will be executed faster than method 1, as even in the worse case scenario where the time complexity is O(N), the N value will always been a smaller number than the N value in method 1 due to the number of passwords being a subsets of the the total nodes thus only checking the password nodes in the graph will run at O(logN) on average where N is the total number of nodes in the graph.

To see the extent of the users usage of multi-factor authentication methods, can be accomplished by finding all the nodes which resemble an account and count the number of edges that were inbound to the node, checking how many items of information is required to access the account. For the account to be classed as using multi-factor authentication the number of information required must fall in line with 2 or more categories of the 'Something I know' (e.g. a password or pincode), 'Something I have' (e.g. Notebook containing passwords) and 'Something I am' (e.g. A thumb or face for biometic authentication) model.

4.1.3 What the user is doing well. Results for this section are a good way to motivate the user by validating their efforts in being secure, with the added bonus that the results can be calculated based on manipulating the results from tests already computed in the previous two sections. For example, checking if the older adult uses a password manager, which accounts have multi factor authentication enabled, and which passwords have are have the strength value of '*strong*' can be found by the same test in performed for the 'Best Practices Issues' section and if the older adult does not reuse a password, and has enabled proper authentication methods to unlock a device can be inferred by the results of the tests in the 'Critical Issues' section.

4.2 Displaying security information and advice to older adults

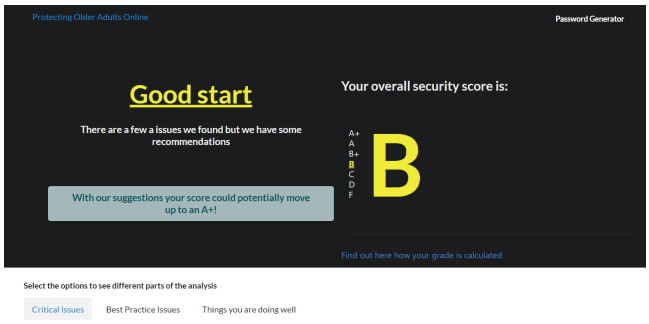

Figure 4: Example of the web application assigning a security grade after analysis

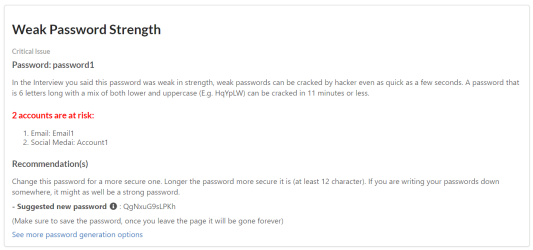

Figure 5: Example of the web application identifying a weak password and providing recommendations

First the older adult is presented with a holistic security grade (A+, A, B+, B, C, D and F) in order to contextualise the effectiveness of their current security practices as see in figure 4. Later specific more detailed issues and information are brought to the older adults attention in order to explain what the each issue is, which accounts are affected and most importantly usable solutions of how to fix the vulnerability as see in figure 5.

4.2.1 Calculating security grades. In this project the security grades were calculated by looking at the results of the tests and analysis mentioned in section 4.1 and 4.2. Results from each of the tests were given a score between 0-7 which was assigned using a grading rubric (see table 1), higher the score .

At the end of the analysis all the scores were summed together to create a total score which was then converting into a percentage by dividing by the 42 (6 tests x 7 points) and multiplying by 100. Finally the percentage was fit in between the corresponding grade boundaries (see table 2)

Standards and best practices within computing change at a rapid pace due to the rate of innovation within the field, this is no different within online security thus another challenge was future-proofing the security grades.

Taking a more inspiration from the UK's EPC system it was made clear to the user that the grade rubric and boundaries could be re-weighted at a later date to reflect the changes of current security

Table 1: Table of Security Analysis Grading Rubric

Tests	Grades						
	A+	A	B+	B	C	D	F
Reused Passwords (% of all passwords)	0%	1-10%	11-25%	26-50%	51-70%	71-90%	91-100%
No. of Accounts Not Using Multi-Factor Authentication (% of all accounts)	0%	1-10%	11-25%	26-50%	51-70%	71-90%	91-100%
Using a Password Manager (Yes/No)	Yes	Yes	Yes	No	No	No	No
Number of Average Passwords (% of all accounts)	0%	0%	1-10%	11-20%	21-50%	51-70%	71-100%
Number of Weak Passwords (% of all accounts)	0%	0%	1-10%	11-20%	21-50%	51-70%	71-100%
Password Protected Devices (% all of the Devices)	100%	100%	100%	100%	99-50%	49-25%	24-0%

Table 2: Table of Security Grade Boundaries

Grades	Boundary
A+	100%
A	90-99%
B+	80-89%
B	70-79%
C	60-69%
D	50-59%
F	0-49%

standards and best practices. For example the standards required of gain a '*B+*' today, could in the future only gain a maximum grade of a '*C*' .

4.2.2 Displaying specific information. The information was split into three sections based on the severity of the security issues: Critical issues, Best Practice Issues and What they user is doing well. Within each of the sections, the order of displaying the information was based on priority, the most important issues were displayed to the user first. This design decision was based on the work by Egelman et al [13] mentioned in section 2.4

Each test result was displayed using a card design. A clear heading about what the issue was, a summary explaining the issue using simple non technical words (based on the the work by Harbach et al [26] and Redmiles et al [44] stating to talk in the language of the user mentioned section 2.4), depending on the issue a clear list of what accounts were specifically at risk due to this vulnerability and finally concluding with a short concise section for recommendations written using key words containing the main parts of the information.

It was fundamental that the information could be implemented only using the advice that was written moreover based on the results seen in section 3.2.5 the key words could be used point the older adults in the right direction if they wanted to take the results further to research the topic in their own time.

For example when advising the older adults on how to implement multi-factor authentication: "*Set up Multi-Factor Authentication for these accounts. This could mean one half of the password are written down somewhere or you get a text with a code to enter or an Authenticator app such as Google Authenticator or Microsoft Authenticator. (Note that SMS based MFA is less secure than an Authenticator App but still better than nothing at all)*" the message is broken up into 3 parts, a short statement on what to do "*Set up Multi-Factor Authentication for these accounts*", the methods of which they should use to implement the advice "*This could mean one half of the password are written down somewhere or you get a text with a code to enter or an Authenticator app such as Google Authenticator or Microsoft Authenticator*" and ending with any caveats the older adults should be aware off when deciding how to use the methods in a way that works for them "*Note that SMS based MFA is less secure than an Authenticator App but still better than nothing at all*".

4.3 Quantifying Security

Based on the results captured during the interviews, the older adults wanted a method to quantify their online security and how effective their efforts were within the context of today's security standards and best practices.

A few methods were considered when deciding how to quantify someone security such as in the form of a numerical score. When looking into what a numerical security score implementation may look like, a major usability issue was stopped. For example do numbers alone give enough information to clearly explain what the user is doing well, what would be the practical difference between someone who scored 75 and someone who scored 78 be? With a difference so close in reality is the latter person really more secure than the other?

Another method that was considered was a letter grading system. Assigning letter grades such as '*A+, B, C etc.*', stemmed from Energy Performance Certificates (EPC) of property in the UK [36]. Using letter grades meant that grade boundaries could be set to group together numerical scores, which in reality would be in a similar situation. This allowed the quantification of the users security to be presenting using a method where differences in grades were clear, intuitive and most importantly reflected translated effectively into reality.

5 OLDER ADULTS AWARENESS OF SECURITY RISKS

In order to evaluate older-adults awareness of their security risks, 5 semi-structured interviews were conducted with participants from our intital user study. Each session lasted between 20 minutes with video-conferencing software used to conduct the interviews. Each interview was conducted by the same person to en-sure coherence and consistency.

The semi-structured interviews had two aims. First, to understand participants personal awareness of their security risks. Second, to allow participants to reflect on the results of the analysis and the impacts it may have to their account ecosystems as a whole.

5.1 Evaluation Materials and Equipment

Demographic Information: All 7 of the original participants were contacted again due to sensitive nature of the account structure information that had to be used to use the system. Everyone other than P3 and P6 from the previous user study decided to take part in the evaluation thus all the participants will be continued to be referred to as their identifiers used in section 3.2.5.

Interview Setup: The semi-structured interview took place using the Zoom Video conferencing software [57].

***Interview Script*:** An interview script was used to maintain a high level of consistency and coherence between all of the interviews. The evaluation script was designed specifically to allow for conversations to flow naturally as any points or views that were brought up could be explored and elaborated due to the scripts semi-structured nature. The evaluation interview script is shown in appendix: I.2

Account Security System: The previously described account structure analysis system was shared with participants during the study. The primary researcher shared their screen with participants in order to provide a soft on boarding experience and to guide participants through the different options that were available in the system. Participants were given an opportunity to reflect on individual points that were brought up and were encouraged to discuss any issues as part of the semi-structured interview process.

Experimental Procedure: The total study took 20 minutes of the participants time. The start of the study each participant was ask questions to check their awareness of their own security as seen mentioned above before seeing the results of the account security system. Once the questions were answered the previously mentioned system was shown to the participants as stated above. After the participants had time to view and understand the results of the analysis the seconds half of the interview questions were asked in order to capture the participants reflections of their current security with regards to the results of the analysis from the account security system.

5.2 Results

All interview sessions were analysed by the author. Every attempt was made to keep interviews impartial however, a potential avenue where bias may be present is that the author was present when each interview session was conducted. Thus a structured interview guide was used to reduce this risk. The interviews were transcribed anonymised and annotated by the author before analysis. Sections of the interviews from all the participants were combined and were inspected individually based on components of the interview guide. Conclusions found within the results are formulated from the trends seen within the data and notable features are also highlighted

5.2.1 Perceptions of the most important and secure accounts within account ecosystems. When classifying which accounts are the most important there are two factors to consider, which account contains the most valuable data and information and secondly which accounts are the most connected within the older adults personal account ecosystems.

P1 and P7 stated their most important accounts purely due to the connectivity within their account ecosystems was their main email account as "*it links to almost all of my accounts*" (P7). However P7 went on to add "*my email account isn't as important as my financial accounts but none the less still very important*" Which was an view that was shared by P2 and P5 who stated their most important account were their financial accounts.

All participants indicated that "*any accounts that handle financial transactions*" (P5) such as a "*bank*" (P4) were the accounts within their ecosystem that required more attention than the other accounts to secure due to the risk of financial loss.

When analysing account access graphs, participants primary email was considered the most important account due to the the connectivity factor as the primary email account was used to create almost every other account used by the participants and could also be accessed using the email as a recovery method.

5.2.2 Awarenesses of their current security vulnerabilities. P2, P4 and P7 stated vulnerabilities that maybe be present were probably passwords related. P4 discussed that they were "*sure the analysis will say something about my devices not being password protected*" and P7 acknowledged that their "*email password may not be as strong as it ought to be*", P4 ended their answer by stating they were "*not sure what to expect really I went in with an open mind*". However P1 and P5 started they were not aware of any security vulnerabilities that were currently present.

Once the analysis results were shown to the participants, P2 was surprised that before they would "*never considered the possibility of my devices being stolen and what they means for my other accounts*" as physical access to their devices meant that any of their accounts could also be accessed, as there was a digital unencrypted file containing their passwords. P7 went on to state "*I wasn't too sure how secure it was to write down my passwords"* referring to the non digital password management strategy of writing passwords down in a notebook, as the passwords that were written down could be unique thus avoiding password reuse and strong as they were not relying on memory to use the password.

For P1 seeing the results validated the efforts and strategies they had in place "*I'm just surprised I did so well ... it's nice to see I'm on the right track* ".

5.2.3 Perceptions and actions of what can be done to increase account security. P2 and P7 indicated that if were they to do anything it would "*probably be changing my passwords to stronger ones*" (P2), which are "up to date with current standards" (P7). P2 went on to add they "*knew it might be an issue at some point but never got around to changing them*", but once seeing the analysis P2 concluded that "*I knew my passwords needed some work but not to this extent, this has been really eye opening ... I will definitely changing all my passwords, right after this actually!*" followed by P7 stating after seeing their analysis "I will definitely have to look into what counts as a strong password in today's standard"

P1 and P5 stated they were "*doing the best I can*" (P1). P5 and P4 said they have "*no idea*" (P4) for the same reason that P1 brought up "*I can't think of anything I could do better*" in order to be more secure.

After the analysis it was brought up that P5 shared a password with a financial account they own and several shopping accounts which lead the reply of "I'll be changing my Paypal passwords as ... it was a bit silly to use the same password for some of my other accounts too"

6 DISCUSSION

The project finding contextualise the account structure and security practices used by older adults by giving an insight to their mindset, habits and practices they choose to implement . We discuss the comparisons of an older adult's security habits with the reality of risks present, current security standards and other demographics.

6.1 Personal Account EcoSystems (RQ1)

When the account ecosystems which were created by older adults are analysed the older adult specific trends start to emerge, susceptibility of scams and fraud, password hygiene, an impact on their account security due to a physical attack and finally the lack of Multi-Factor Authentication methods.

Previous research shows that older adults tend to be at a greater risk of becoming a victim of cyber crime such as scams and fraud [35] than younger demographics, the results of the studies conducted show that these threats creates an atmosphere and mindset within the older adults to be caution and suspicious when ever online. The demographic that is was interviewed throughout this project are without doubt the most at risk of becoming a target to cyber criminals as the participants use the internet more frequently and extensively than others within their demographic. On average the participants have 12 accounts that are in active use thus increasing the area where an attack could take place.

Even though the participants are most at risk are uncovered during the semi-structured interviews throughout this project the older adults also have their own effective strategies in place when it comes to protecting themselves from becoming a victim. As found through the interviews conducted, older adults tend to use password management strategies both digital and non digital. The majority of the older adults use non digital unencrypted password management techniques, such as writing passwords down in a diary. Doing so lowers the older adults risk of reusing passwords and increases the chances of a complex password being used, as memory is not a factor in play which goes against the trends seen by other demographics as shown by NIST, where a user creates a password so overly complex that it is forgotten thus replaced with a weaker alternative [19].

Basing security practices on memory alone creates other avenues where the older adults could be at risk. It was discovered when analysing of the older adults personal ecosystems that the a considerable risk to their online security could originate from physical risks. If a device was stolen from an older adults it would give access to all the accounts within their ecosystem. Often it was found that participants either did not have proper authentication methods enabled on their devices as seen in the account graphs of P4 and P7 or that the information required to unlock a device would also give the attacker access to the older adults password manager as seen in the case of P3 where the password required to unlock the '*device4*' is the same passwords required to access the their digital encrypted password manager, or in the case of P2 where once the attacker bypasses the password for '*device1*' (which was referred to as weak in strength by the participant) the attacker would have access to an unencrypted password-less file used to manage their passwords.

Muti-Factor Authentication is a security practice that is not used widely throughout the ecosystems of older adults. A trend that is present in every account ecosystem where multi-factor authentication is enabled is that the practice is only ever implemented when it is mandatory such as a finance account as seen in the account graph of P1, P2, P4 and P7.

6.2 Differences between perceived awareness of account security and current security vulnerabilities RQ2

The older adults have shown their mindsets and awareness to their own account security throughout the user studies in this project. When comparing the older adults perception of their security and reality of the situation, the two are not far off from each other. The results of this project found 4 noticeable areas, the self risk assessments that older adults must make, password strength and making the most of their password management techniques, views on replying on 3rd parties and finally their perceptions of where the greatest risks to their account security are.

Each of the older adults in their own way are victims of expectation to use unusable security practices or practices that are not fit for purpose when considering the needs and situations of the older adults. The older adults must make self risk assessments to gauge if the protections they will acquire from a new security practice is worth the effort to implement and alter their mental security model. As found in the the studies above usability of the practice, understanding of what the practice is and how it affects their mental model of security and finally trust the practice is sound and secure are the fundamental barriers that must be accounted for when when the older adults is deciding to implement a practice or not.

It was found that all the older adults interviewed have implemented a password management strategy both digital and non digital. This is a good start as the older adults are aware of the risks attached to reusing passwords thus go out of their way to ensure each password is unique. However not all of the strategies are being used to their full potential. For example it was found that one participant's technique to create unique passwords were to create permutations of a base password. In reality this strategy creates a false sense of security. Once an individual password is broken a trend can quickly be identified thus the attacker could use a throttling brute force attack to find the other permutations potential passwords which could be used for other accounts. Another item that could be implemented to make the most of their password management techniques are writing down strong passwords as the results of the security analysis found that on average more than 70% of the passwords used by the older adults were potentially not to current day standards proposed by NIST [19]. The older adults are not relying on memory to access a password thus it would be beneficial that if the passwords that are written down conform with validated password creation methods such as are set of complex random characters at least of length 12 [19] .

The view of trusting 3rd parties to protect them are split according to the older adults. There are some who state that the 3rd parties you trust with your sensitive information have a duty to maintain the confidentiality of the information, however some state that the

full responsibility and control must sit with them. It was found that a commonality between both mindsets stem from trust, the older adult only give away information if they trust the 3rd party this can be clearly seen in the account graphs created by the older adults the average number of accounts that are in active use is 12 which to be much lower than the account graphs of other demographics found in the original research by Hammann et al [23] or the average 16-26 of accounts a person has [15, 40, 41, 55].

It was also found that a number of the older adults initial perceptions of which accounts were the most important to secure came down to what valuable data and information that account held such as financial accounts. When reflecting this view with the analysis results it was found that the older adults banking accounts were the most secure within the whole account ecosystem, how ever the most important account that was identified was the older adults primary email. As all the account the older adults had were linked by their email address. Looking at the bigger picture the email account could be used as a recovery method to access every account to was linked to within the ecosystem. Thus it was recommended that the email address should be the account that is the most inconvenient for an attacker to compromise, such as use a very strong password and enable multi-factor authentication.

7 CONCLUSION

The project was designed to support older adults to defend and more importantly, provide independence to protect themselves from cyber attacks compromising their account security. The project set out to investigate the following two questions:

- RQ1 What do personal account ecosystems created by older adults look like?
- RQ2 What differences exist between older adults' perceived awareness of account security and current security vulnerabilities?

This research was motivated and justified through a review of literature in the areas related to account security, usable security and the securing of older adults online.

Two user studies were conducted the first set of semi structured interviews involving 7 older adults aimed to capture the account structure information to classify trends and features within a personal account ecosystem created by an older adult as well as to gain an insight into the older adults mindset regarding account security and the practices that are implemented. The second user study was a set of semi-structured interviews with 5 older adult to understand what the older adults perceive as their current risks compared to what the actual risks present in reality are.

To compare the older adults perceived risks with the reality of risks present and to investigate the effectiveness of their current security practices a web application was created to analyse the account structure information to find vulnerabilities and provide appropriate solutions in order to empower the older adult in taking a closer step in becoming secure online.

The findings of the user studies led to the creating 7 account access graphs modelling the personal account ecosystems created by older adults which was combined together to create the first dataset of older adults account structure information. Within this dataset clear trends and similarities were identified such as a typical account access graph created by an older adults has 33 nodes and 59 edges where only 12 on average are accounts that are in active use. It also was found that within all the account access graphs the older adults primary email address was the most critical node due to the email being used to create every other account and recovery options available.

The study tackles the narrative that older adults are insecure online as it is found that older adults in the user studies are more weary and careful when it comes to being online such as trusting websites or clicking links. It was found that the perceptions of security was not far of from the reality of the situation, that the older adults tend to be more suspicious when online, and will research topics extensively before implementing.

Which justifies why a security practice must conform to 3 key factors: Usability, Trust, and Understanding for an older adult to consider adopting the practice. This often leads to older adults altering security practices to work them for them. Such as using both digital and non digital password management techniques such as a text file or a notebook to store their passwords in order to avoid password reuse.

Due to the lack of understanding and trust a trend that is also commonly seen was the minimal use of multi-factor authentication, the practice was only ever being used on accounts where it was mandatory.

7.1 Limitations

The user studies were conducted using 7 and 5 older adults, this sample is therefore not a full representation of all older adults aged 70+ due to the number of participants, though this should not take away from the fact that this is the first study conducted focusing on older adults in relation to account security.

All the participants were recruited from the 'Bytes and Blether' group part of the User Centre located at University of Dundee. This is an initiative by the university to teach technological literacy to older adults, thus all the participants have access to relatively good resources and information on using technology as well as have some what of an awareness of cyber security and privacy issues.

7.2 Generalisations and Future Work

Accounts make up so much of our digital identities (if not all) protecting our accounts is in everyone's best interest. There is a need for work in automatically protecting peoples digital identities in order to provide a real time analysis of vulnerabilities that pop up.

Work on finding issues and presenting account security information and modifications is a big part of being secure especially in the times of cyber warfare we live in now. The argument of '*I'm not important, I won't be attacked so I don't need to worry*' is no longer valid. The risk of an individual being personally attacked is low **but** the risk of the same individual being the weakest link in the supply chain is high thus the point an adversary attacks as part of a bigger goal.

General security monitoring and recommendations: This project also brings to light a few areas worth further investigation. Such as a personalised security analysis for other demographics other than just older adults where the feedback provided can adapt to the needs and context of the user.

Protecting older adults: Finally there is still work to do when protecting older adults when online. Consideration if an older adult can effectively implement the practice must be done by reflecting and investigating if the tool or practice complements the mindset and strategies used by older adults in regards to usability, trust and understanding.

8 ACKNOWLEDGMENTS

I would like to thank Dr Michael Crabb, for his support throughout this project and pushing me outside my comfort zone allowing me to explore, create and learn. His superb guidance has without a doubt pushed the project and my self to develop far greater than originally could be imagined.

Secondly I would also like to thank Dr Saša Radomirović for showing his continued interest in my project and providing his expert insight when asked.

Thirdly I would like to thank Kamila Gorska for her undoubted support both within and outwith the project.

I would also like to thank Mrs Kathleen Cummins for her exceptional help in supporting me through the process of finding participants and introducing me to the User Centre.

Finally I give my thanks to the participants who took part in my project and the User Centre for giving me an insight into the challenges that exist for older adults using technology but more importantly showing me how inaccurate the stereotypes which exist about older adults are.

REFERENCES

[1] Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *22nd {USENIX} Security Symposium ({USENIX} Security 13)*. 257–272.

[2] Linda M Alves and Steve R Wilson. 2008. The effects of loneliness on telemarketing fraud vulnerability among older adults. *Journal of elder abuse & neglect* 20, 1 (2008), 63–85.

[3] Keith B Anderson. 2004. *Consumer fraud in the United States: An FTC survey*. Federal Trade Commission Washington, DC.

[4] Iman Azimi, Amir M Rahmani, Pasi Liljeberg, and Hannu Tenhunen. 2017. Internet of things for remote elderly monitoring: a study from user-centered perspective. *Journal of Ambient Intelligence and Humanized Computing* 8, 2 (2017), 273–289.

[5] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. 2013. Your attention please: Designing security-decision UIs to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*. 1–12.

[6] Jean Camp and Kay Connelly. 2008. Beyond consent: privacy in ubiquitous computing (Ubicomp). *Digital privacy: Theory, technologies, and practices* (2008), 327–343.

[7] Brian D Carpenter and Sarah Buday. 2007. Computer use among older adults in a naturally occurring retirement community. *Computers in Human Behavior* 23, 6 (2007), 3012–3024.

[8] Michelle Caruthers. 2018. World Password Day: How to Improve Your Passwords. https://blog.dashlane.com/world-password-day/

[9] Michael Crabb, Rachel Menzies, and Annalu Waller. 2020. The User Centre. (2020).

[10] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The tangled web of password reuse.. In *NDSS*, Vol. 14. 23–26.

[11] Frederik De Keukelaere, Sachiko Yoshihama, Scott Trent, Yu Zhang, Lin Luo, and Mary Ellen Zurko. 2009. Adaptive security dialogs for improved security behavior of users. In *IFIP Conference on Human-Computer Interaction*. Springer, 510–523.

[12] Kerry Dobransky and Eszter Hargittai. 2016. Unrealized potential: Exploring the digital disability divide. *Poetics* 58 (2016), 18–28.

[13] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1065–1074.

[14] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. 2017. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences* 7, 1 (2017), 1–20.

[15] Dinei Florencio and Cormac Herley. 2007. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*. 657–666.

[16] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. 2016. Do or do not, there is no try: user engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*. 97–111.

[17] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*.

[18] Google. 2021. Google Identity. https://developers.google.com/identity

[19] Paul A Grassi, James L Fenton, EM Newton, RA Perlner, AR Regenscheid, WE Burr, JP Richer, NB Lefkovitz, JM Danker, Yee-Yin Choong, et al. 2017. NIST special publication 800-63b: digital identity guidelines. *National Institute of Standards and Technology (NIST)* (2017).

[20] Galen A Grimes, Michelle G Hough, Elizabeth Mazur, and Margaret L Signorella. 2010. Older adults' knowledge of internet hazards. *Educational Gerontology* 36, 3 (2010), 173–192.

[21] Galen A Grimes, Michelle G Hough, and Margaret L Signorella. 2007. Email end users and spam: relations of gender and age group to attitudes and actions. *Computers in Human Behavior* 23, 1 (2007), 318–332.

[22] Miguel Grinberg. 2018. *Flask web development: developing web applications with python*. " O'Reilly Media, Inc.".

[23] Sven Hammann, Saša Radomirović, Ralf Sasse, and David Basin. 2019. User account access graphs. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 1405–1422.

[24] Vicki L Hanson. 2011. Technology skill and age: what will be the same 20 years from now? *Universal Access in the Information Society* 10, 4 (2011), 443–452.

[25] SM Taiabul Haque, Matthew Wright, and Shannon Scielzo. 2013. A study of user password strategy for multiple accounts. In *Proceedings of the third ACM conference on Data and application security and privacy*. 173–176.

[26] Marian Harbach, Sascha Fahl, Polina Yakovleva, and Matthew Smith. 2013. Sorry, I don't get it: An analysis of warning message texts. In *International Conference on Financial Cryptography and Data Security*. Springer, 94–111.

[27] Dominik Hornung, Claudia Müller, Irina Shklovski, Timo Jakobi, and Volker Wulf. 2017. Navigating relationships and boundaries: Concerns around ICT-uptake for elderly people. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 7057–7069.

[28] Blake Ives, Kenneth R Walsh, and Helmut Schneider. 2004. The domino effect of password reuse. *Commun. ACM* 47, 4 (2004), 75–78.

[29] Sophie Nicholls Jones. 2018. Seniors too ashamed to report financial fraud, say experts. https://www.cpacanada.ca/en/news/canada/2018-06-15-seniors-too-ashamed-to-report-financial-fraud

[30] Jake Knapp, John Zeratsky, and Braden Kowitz. 2016. *Sprint: How to solve big problems and test new ideas in just five days*. Simon and Schuster.

[31] Bran Knowles and Vicki L. Hanson. 2018. The Wisdom of Older Technology (Non)Users. *Commun. ACM* 61, 3 (Feb. 2018), 72–77. https://doi.org/10.1145/3179995

[32] Nicole M Lee. 2018. Fake news, phishing, and fraud: a call for research on digital media literacy education beyond the classroom. *Communication Education* 67, 4 (2018), 460–466.

[33] Nick Leiber. 2018. How Criminals Steal 37 Billion a Year from America's Elderly. https://www.bloomberg.com/news/features/2018-05-03/america-s-elderly-are-losing-37-billion-a-year-to-fraud

[34] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song. 2014. The emperor's new password manager: Security analysis of web-based password managers. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)*. 465–479.

[35] Nigel Martin and John Rice. 2013. Spearing high net wealth individuals: the case of online fraud and mature age internet users. *International Journal of Information Security and Privacy (IJISP)* 7, 1 (2013), 1–15.

[36] Stephen Maunder. 2019. Expert testing, reviews and advice from Which? https://www.which.co.uk/money/mortgages-and-property/home-movers/selling-a-house/epcs-explained-a6nmp1q099fb

[37] James Nicholson, Lynne Coventry, and Pamela Briggs. 2019. " If It's Important It Will Be A Headline" Cybersecurity Information Seeking in Older Adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–11.

[38] Chris Norval, John L. Arnott, and Vicki L. Hanson. 2014. What's on Your Mind? Investigating Recommendations for Inclusive Social Networking and Older Adults. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. Association for Computing Machinery, New York, NY, USA, 3923–3932. https://doi.org/10.1145/2556288.2556992

[39] Nord Pass. 2021. Press area for journalists and media outlets. https://nordpass.com/press-area/
[40] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. 2017. Let's go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 295–310.
[41] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. In *Fifteenth Symposium On Usable Privacy and Security (SOUPS 2019). USENIX Association, Santa Clara, CA*. 319–338.
[42] Sebastiaan TM Peek, Katrien G Luijkx, Maurice D Rijnaard, Marianne E Nieboer, Claire S van der Voort, Sil Aarts, Joost van Hoof, Hubertus JM Vrijhoef, and Eveline JM Wouters. 2016. Older adults' reasons for using technology while aging in place. *Gerontology* 62, 2 (2016), 226–237.
[43] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J Aviv. 2020. Why Older Adults (Don't) Use Password Managers. *arXiv preprint arXiv:2010.01973* (2020).
[44] Elissa M Redmiles, Everest Liu, and Michelle L Mazurek. 2017. You Want Me To Do What? A Design Study of Two-Factor Authentication Messages.. In *SOUPS*.
[45] Andrew Sears and Julie A Jacko. 2009. *Human-computer interaction: design issues, solutions, and applications*. CRC Press.
[46] CACM Staff. 2016. React: Facebook's functional turn on writing Javascript. *Commun. ACM* 59, 12 (2016), 56–62.
[47] Amber Steel. 2017. LastPass Reveals 8 Truths about Passwords in the New Password Exposé. http://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose/
[48] Elizabeth Stobert and Robert Biddle. 2014. A password manager that doesn't remember passwords. In *Proceedings of the 2014 New Security Paradigms Workshop*. 39–52.
[49] Bethany Tennant, Michael Stellefson, Virginia Dodd, Beth Chaney, Don Chaney, Samantha Paige, and Julia Alber. 2015. eHealth literacy and Web 2.0 health information seeking behaviors among baby boomers and older adults. *Journal of medical Internet research* 17, 3 (2015), e70.
[50] Age UK. 2020. Computer training courses - IT training services. https://www.ageuk.org.uk/services/in-your-area/it-training/
[51] Grand View Research. 2018. Password Management Market Size, Share & Trends Analysis Report By Type, By Access Type (Desktops, Mobile Devices), By Organization Type (BFSI, Healthcare), By End-User Type, And Segment Forecasts, 2018 - 2025.
[52] Kerryellen G. Vroman, Sajay Arthanat, and Catherine Lysack. 2015. "Who over 65 is online?" Older adults' dispositions toward information communication technology. *Computers in Human Behavior* 43 (2015), 156 – 166. https://doi.org/10.1016/j.chb.2014.10.018
[53] Nicole Wagner, Khaled Hassanein, and Milena Head. 2010. Computer use by older adults: A multi-disciplinary review. *Computers in human behavior* 26, 5 (2010), 870–882.
[54] Chun Wang, Steve TK Jan, Hang Hu, Douglas Bossart, and Gang Wang. 2018. The next domino to fall: Empirical analysis of user passwords across online services. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*. 196–203.
[55] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. 2016. Understanding password choices: How frequently entered passwords are re-used across websites. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*. 175–188.
[56] Michael S Wogalter. 2006. Purposes and scope of warnings. *Handbook of warnings* 864 (2006).
[57] Zoom. 2021. Video Conferencing, Web Conferencing, Webinars, Screen Sharing - Zoom. https://zoom.us/

A SYSTEM DESIGN

A.1 Development Methodology

This project took on a hybrid approach between two of the methodologies which are commonly used in software development: the Waterfall and Agile approaches. Aspects from the Waterfall methodology that were taken advantage of was setting a as clear project end date and that the project saw itself move into defined phases: Requirements, Design, Implementation and Evaluation. Due to the hard deadline, the project was required to keep progressing into the next phase on schedule which is where attributes from the Agile Methodology are utilised. The project handled change by dynamically moving between phases to fix and reevaluate elements that were created in different phases or issues that arose ad hoc.

The requirements gathering and creation phase was accomplished using user storied in the form of "*As a <name>, I want <feature/requirement> in order to <rationale>*". This allowed for a product backlog to be created and the user stories to be split using the MoSCoW prioritising technique used in agile to create the critical path, which highlights the main user storied where their completion is relied on by all the other user stories in order for the project to be developed.

Another step that was taken was after the first user study which aimed to understand older adults and their needs user personas were created (which can be viewed at appendix L), in order to understand the user and build a sense of empathy towards the needs and context of the older adults as well as any secondary actors that would be affected by design decisions.

Once the personas were complete a condensed design sprint was conducted inspired by the book '*Sprint: How to solve big problems and test new ideas in just five days*' by Jake Knapp [30]. The Main goals were to generate ideas and solutions quickly, thus during this stage low fidelity designs were created quickly on medium such as post it notes, whiteboards and paper. Once a central idea was identified 3 medium fidelity design was created using Figma an online design tool created for prototyping. Next elements of all 3 designs were merged into one final high fidelity concept created using Adobe XD in order to assess and curate the user experience while using the web application.

During the development phase of the project Jira was used as a project management tool in order to store the user backlog and manage development sprints. The total development of the web app was completed within 2 and a half week long sprints which is explained in detail in appendix B.

The web application was evaluated through an evaluation user study using a survey. Please see appendix C.2 for more detail on the usability testing conducted of the web application.

A.2 Design Decisions and Alternatives

To analyse the account structure information a web application was decided to be created, in order to removed a barrier where the analysis could only be viewed and accessed using specific hardware if the analysis was a software program.

Another reason was that double the work load would be created to make the program compatible for both the Windows operating system and Mac OS. A possible solution could be to save the time and effort of created multiple code bases for different operating

systems was a Progressive Web App (PWA) implementation. However, it was decided to be out of scope and an inefficient use of time as created a PWA, a web application would also be created as a consequence, thus would be it would be more efficient and have a wider reach to the target user if the application could only be accessed using the internet.

Due to the project being a web application, it was built to be responsive and adept based on screen size. This allowed for the older adult to access the analysis using any device as long as it held the original account structure information JSON file. This was another advantage of not created a desktop program as the analysis could be viewed anywhere as long as the older adult had an internet connection than only using the device where the software was installed.

The justification was that the physical process of accessing the analysis was easier due to the creation of a web application as the older adult would only need to open a browser, go to the analysis website and upload the account structure file. Opposed to the older adults needing to go to the website where the software can be downloaded, download and install the program and then finally upload the account structure file. Thus the processing of accessing the analysis was still available to those who may not have had the sufficient digital proficiency.

A.3 Technologies

A.3.1 React. React is an open source Javascript library created by Facebook in 2013 specifically to support building user interfaces. Other alternatives were considered such as Angular and View js however, React was ultimately chosen to create the front end of the web application as React is a library not a framework such as Angular or View thus allowing for greater flexibility when working with other libraries if required and ultimately having more freedom and control within development than conforming to a frameworks standards. Another factor which lead to React being chosen was the authors inexperience using the library and paradigm as the author could build proficiency by getting '*hands on*' experience using the library.

A.3.2 Python. Python is considered as a high level programming language where the code is executed by an interpreter. Python was chosen as the main back end language for this project yet other alternatives were also considered such as PHP, Java or not using a back end at all thus processing everything client side using Javascript and WebAssembly. The main reason for choosing python was the account structure data was stored in a JSON file, it was clear that due to the similar syntax between JSON and python's standard dictionary data structure that python would be the most appropriate to use in order for the seamless conversion between the two languages. Another factor which excluded PHP and Java from consideration was the author had already developed web applications using the two languages before thus there would be no learning experience.

A.3.3 Flask. Flask is a micro web framework built to support the usage of python as a back end language. Flask allows for a Modal View Controller (MVC) pattern to be built with ease as an API can be in order for the front end to communicate with the back end and vise versa. Another library considered was Django, but Flask was ultimately chose due to the frameworks RESTful request dispatching capabilities allowing for end points to be created and data to be transferred efficiently, a feature with Django cannot handle gracefully.

A.4 Tools + Software

A.4.1 Visual Studio Code. Version 1.55.1 was used as the main code editor to develop this project.

A.4.2 GitHub. Used as source code management.

A.4.3 Heroku. Service used for Hosting the web application.

A.4.4 Account Access Interview Tool. Was used to create the account access graphs.

A.4.5 Mircosoft Word. Used during the user studies to write notes.

A.4.6 Mircosoft Excel. Used during the project to manipulate data and time management.s

A.4.7 Atlassian's Jira. Was used during the development phase of the project to track user stories and organise sprints.

A.4.8 Overleaf. A LaTeX editor used to write the midterm and final report.

A.4.9 Jisc. Was used to create the evaluation surveys.

A.4.10 Figma. Used to create low/medium fidelity prototyping.

A.4.11 Adobe XD. Used to create a high fidelity prototypes and explore user experience.

A.5 Acquisition of New Knowledge and Skills

There were ample opportunities for the author to pick up new knowledge and skills throughout the project. Firstly the project being individual allowed the author to gain more experience doing all the tasks that would normally be spread out over a group of people. A lot of the project was '*swimming in the deep end*' thus new skills and knowledge were picked up and applied quickly. The skills and knowledge that have been acquired can be split into two distinct categories.

A.5.1 Technical. The author previously had limited knowledge and experience using Python which was the language the whole backend was written in thus a large portion of time was dedicated in learning the language. On top of Python the author had never creating an API to communicate between both front and backend thus research went into learning Flask to facilitate the communication between the React frontend as well as the Python backend

The author had previously used an older version of React once before. However, the current standards within react have been updated since then having completely changed thus the experience was similar to picking the library up for the first time, which allows the author to learn modern day Javascript standards (ECMAScript 2018).

Through creating each layer of the web application the author gained an understanding of the work and responsibilities of each layer within a web stack to see how each of the layers work with each other harmoniously together.

A.5.2 Non-Technical. One of the key skills the author learned throughout the project was how to conduct a literature review of a topic effectively using tools such as Google Scholar to find, traverse and understand academic papers. Similarly the author picked up insight into how to effective read an academic paper critically.

The author gained experience in academic writing in terms of the standards required, the structure to present information as how to communicate data and thought effectively such as referencing facts and information when declared as well a the different methods to gather and present quantitative and qualitative data.

Finally the last academic skill that was acquired was how to identify trends and features with large sets of data accurately without potentially compromising the results with bias.

B DEVELOPMENT SPRINTS

Product and Sprint backlogs were created and tracked using Jira, an agile project management tool created by Atlassian. The Product backlog contained User Stories written using the format 'As a <actor>, I want to <feature/requirement> in order to <rationale>'. For every story a priority level was assigned ranging from:

- Highest - A story that was on the critical path, if not complete the project could not continue.
- High - Story out with the critical path by the bare minimum features.
- Medium - Story that is important but not critical nor the bare minimum.
- Low - Story that is nice to have if there is time but not important (low effort)
- Lowest - Story that is nice to have if there is time but not important (high effort)

As well as applying MoSCoW ratings:

- Must - Every feature on the critical path and bare minimum features (Highest-High Priority)
- Should - Features that are can only be completed once the 'Must' features are complete (Medium Priority)
- Could - Anything extra that is nice to have (Low Priority)
- Wont - Issues that are very low impact but require a lot of time and effort (Lowest Priority)

B.1 User Story Requirements

(1) As a security expert, I want to see where passwords are being reused automatically in order to spot the security issue quickly without having to spend time on a task that is tedious to do by hand.
(2) As a security expert, I want to see if an account requires multi-factor authentication to be accessed in order to quickly spot the use of a security best practice.
(3) As a security export, I want to see where the critical attack points are in order to allow me to give advice on the most critical issues.
(4) As a older adult, I want access to this the personalised security information any time after the initial interview without a security expert needing to be present in order to be able to go through the information in my own time and read carefully.
(5) As a older adult, I want to be able to print out the security analysis in order to have a non digital version I can keep for reference.
(6) As a older adult, I want to be able to see where I need to improve my account security in order to be aware of the issues I face regarding my online security.
(7) As a older adult, I want to be able to see if the security strategies I am using are successfully keeping me secure in order to see what I am doing well and to validate the implementation of the strategies are correct.
(8) As a older adult, I want to be able to quantify how secure my personal account ecosystem is in order to build a clearer mental modal of my account security.
(9) As a older adult, I would like to know what the potential solutions to my security issues are in order to carry out the steps to improve my account security.
(10) As a older adult, I would like to see what the current best security practices are in order to stay up to date on what the current standards are.
(11) As a family member, I want to see the advice given to my relative is legitimate in order to protect my relative from becoming more vulnerable.
(12) As an older adult I would like to see what the implementation of advice would mean for my security grade, in order to see the impact of each advice.
(13) As a security expert, I want to generate and suggest a new unique password when a weak or average password is identified in order to give the older adult a strong password that is compliant the NIST password guidelines.
(14) As a developer, I need to be able to send the account access interview data to the server in order to process the data.
(15) As a developer, I need to be able to send the analysed data from the server to the frontend in order to visualise the analysis.
(16) As a developer, I need to be able to establish the method to display the analysis from the server to the webapp in order for the display process to be streamline, uniform and modular.
(17) As a developer, I want to process the access interview data as a graph data structure in order to lower the time complexity and stop wasteful looping of data.
(18) As a security expert, I want to find the passwords that the user defined as weak, in order to suggest tips on how to select a more secure password.
(19) As a security expert, I want to show the user the accounts/nodes involved when showing a vulnerability, in order to describe the issue when I am not there.

The Sprints were setup using a basic Kanban layout, split into 3 categories: To-do, In Progress and Done.

The goals and objectives of each sprint were identified based on the priorities and MoSCoW ratings of the user stories in the product backlog. The only software development that was done outwith the sprints were tutorials and Spikes to learn the frameworks and libraries used.

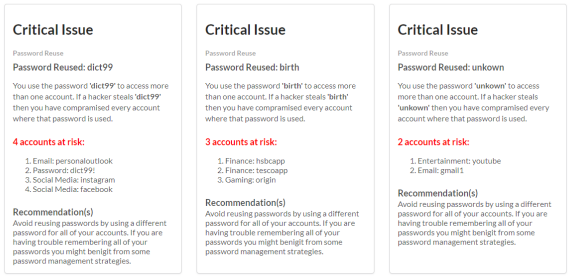

Figure 6: Showing the critical issue of reusing passwords

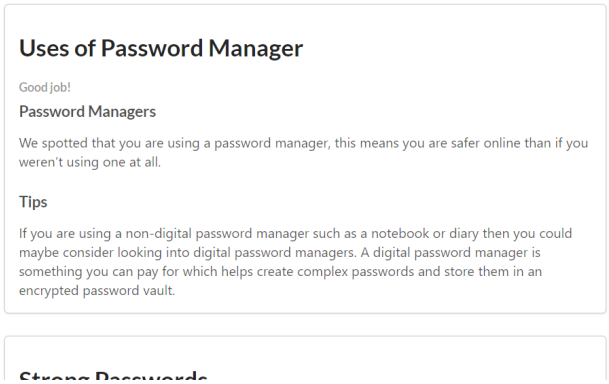

Figure 7: Validating the user in using a password manager

B.2 Sprint 1

Dates: 20/03/21 - 26/03/21 (7 days) **Goals:** The main goals of the first sprint was to complete all the Critical and Highest priority user stories. The goals were based on formatting the JSON input data from the account access interview into a workable format in python; connecting and communicating between both the React Front-end and Flask Python Back-end; processing the account access data to start finding vulnerabilities.

Outcomes: All of the critical and highest priority user stories were completed. The Webapp allows for a personalised analysis by allowing the user to upload their account structure data that was created during their account access interview. To allow for communication between front and back end a Python Flask REST API was created. React would send HTTP GET and POST requests to specific end points within the Flask API. An example of a POST request sending the JSON data to be analysed and receiving the analysed data can be see below:

```
useEffect(()=> {
    fetch("/analysis",{
        method: "POST",
        headers: {
            "Content-Type": "application/json"
        },
        body: JSON.stringify(graph)
    }).then(res => {
        if (res.ok){
            return res.json()
        }
    }).then(data => {
        setAnalysis(data)
        setReached_Data(true)})
},[graph])
```

A modular and streamline method to to visualise the data from the analysis was created by taking advantage of the Components features within React see Figure 6. Data could be passed dynamically straight from the analysis data.

Originally the data from the interview was held in a hash table which required multiple inefficient loops o traverse the data which lead to high time complexities to combat this the data was converted into a graph data structure in python made from scratch using dictionaries and arrays holding keys of the edges going out from the node and keys of edges coming into to the node. This allowed for many of the features to be completed faster and requiring less computation.

For example when detecting if a password is being reused, instead of looping over every account to see if the password is present and doing so for every password the user has. It is as simple as looking at all the nodes that are passwords and seeing if they have more than one edge coming out from the node. If there is more than one edge leaving the node then it is clear the password is being reused to access multiple accounts as a non reused password should only have one edge leaving the node.

As the same for all the nodes that were declared by the user as not strong passwords. They too were found by visiting every node that was a password and checking their strength field. Passwords with a weak strength were grouped together in order to bring up to the user. Passwords that weren't weak but not generated by a password manager were classed as 'Average' and grouped together.

B.3 Sprint 2

Dates: 28/03/21 - 03/04/2021 (7 days) **Goals:** The main goals of the second sprint was to complete the tests used to analyse account structure information then create a method to quantify the users security with the context of current day standards and practices.

Outcomes: All of the user stories that related to analysing the account access information was complete. All High priority user stories and stories tagged as '*Should*' were completed.

The account analysis results were split into 3 sections, critical issues, best practice issues and what the user is doing well in order to reduce the volume of information being displayed to the older adult at one time, which lowers the cognitive load of the user. Splitting the analysis by severity conforms to the research found within the related work section.

One analysis that was created was to identify the most critical node within the account access graph. This user story was accomplished by traversing through the nodes in the graph to find the node which was the most inter connected in terms to the highest number of outbound edges.

Another analysis was to find out to which extent the user incorporates multi-factor authentication (MFA). The accounts which

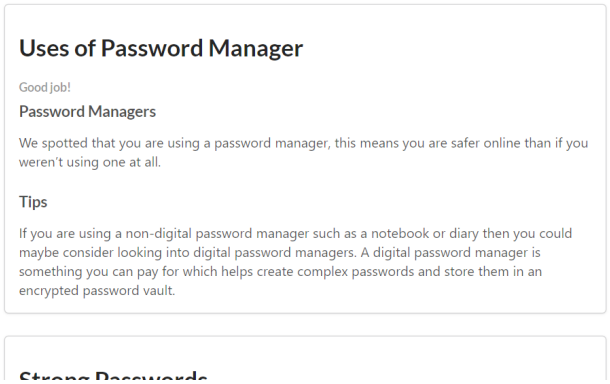

Figure 8: A secure method to generate passwords

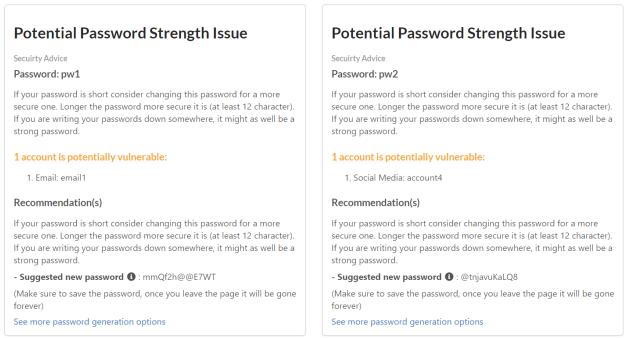

Figure 9: Identifying passwords that may potential not be to standard

are not protected by multi-factor authentication were identified by finding all the nodes within the graph that represented online accounts and counting the number of nodes required to access the node if the number was greater than 2 (email/ username and a password) then the account could be classes as using MFA.

One important part of the project was to provide usable solutions to the vulnerabilities found. The process of coming up with usable solutions the results of the first user study and the user personas were refereed to heavily in order to understand the needs to the older adult to come up with methods that works for them.

To calculate what the user was doing well came down the results of the tests to find what they were not doing well. Such as if the user had a password manager, the accounts with used MFA, which passwords were secure, if the user was reusing passwords or not and which devices were password protected.

The important part was to validate the older adult in order to show them how well they are doing to empower them to go the extra mile. One example was when showing the user what they did well, an extra message was added on what further strategies they could use to take their current strategy and go a fit further. As seen in figure 7 stating "If you are using a non-digital password manager such as a notebook or diary then you could maybe consider looking into digital password managers. A digital password manager is something you can pay for which helps create complex passwords and store them in an encrypted password vault."

A users security grades were a quantified representation of the effectiveness of the security practices and vulnerabilities present. As stated above it was decided that the results of each analysis would be given a score from 0-7, then the scores are accumulated together in order to create a total score which is placed within grade boundaries.

B.4 Sprint 3

Dates: 3/04/21 - 07/04/2021 (5 days) **Goals:** The main goals to complete the final touches to the website such as add text explaining the website and any features that were tagged as '*Could*' or low priority.

Outcomes: All of the user stories that were in scope were completed as well as getting the website hosted.

During the final sprint the final touches of the website were added such as explaining to the user on the home page what the project was about and how the analysis works.

A final check was complete that every result of the analysis was displaying the correct information that all the placeholder text was removed.

As found during the first user study, older adults tend to write them passwords down on in a notebook or a digital file in order to remember passwords and not reuse any of them. Based on this idea a user story was created to supply the older adults with secure passwords when a weak or average strength password was identified as if they were going to write down passwords it might as well be secure ones.

This was accomplished by creating a secure password generator as seen in figure 8. The key features of this password generator was the user could configure the length and characters present. Also by default the password length was set to 12 due to the current NIST standard that passwords would be at least 12 characters long [19] as a subtle method to push the older adults to use passwords that were to NIST's standards.

Another consideration when generating secure passwords was ambiguous letter and characters. As the passwords were probably going to be written down characters such as "I", "l" , "1", "0", "o", "O", etc were removed in order to prevent confusion when reading the password back.

A security concern was to not leak the passwords used by the older adults, the older adults new secure password would not be leaked as it is not saved by generated on demand. Thus if an adversary stole the account structure file and upload it into the web application they would not see the same passwords that were supplied to the older adult originally as seen in the warning at the bottom of figure 9

C SYSTEM USABILITY TESTING

As described above, a web application was created in order to analyse the account structure information to evaluate the security practices and provide recommendations that were useable for an older adult. This web application evaluated by older adults through a survey where the focus was on the systems usability and effectiveness as well as any feedback or improvements for future work.

Table 3: Evaluation Survey results table

Question	Options	Average Response
2.1. The information was explained clearly	Strongly Agree to Strongly Disagree	5 (Strongly Agree)
2.2. The website was intuitive to use	Strongly Agree to Strongly Disagree	4 (Agree)
2.3. It is clear to me what my most important account is	Strongly Agree to Strongly Disagree	5 (Strongly Agree)
2.4. It is clear to me what my security issues are	Strongly Agree to Strongly Disagree	5 (Strongly Agree)
2.5. The solutions for each security issue are presented clearly	Strongly Agree to Strongly Disagree	5 (Strongly Agree)
2.6. It is clear to me what i am doing well currently to keep myself secure	Strongly Agree to Strongly Disagree	5 (Strongly Agree)
2.7. I am very likely to act on this information that was provided in the analysis	Strongly Agree to Strongly Disagree	4 (Agree)
2.8. If I wanted to research more into the analysis that was provided on my own I would know which direction to look.	Strongly Agree to Strongly Disagree	5 (Strongly Agree)
2.a. Do you see yourself revisiting this analysis?	Yes or No	1 (Yes)

C.1 Evaluation Materials and Equipment

Demographic Information: To evaluate the system implementation all 7 of the original participants of the first user study were contacted again due to sensitive nature of the account structure information that had to be used to evaluate the system. Everyone other than P3 from the previous user study decided to take part in the evaluation.

Survey Setup: The survey was a mixture of multiple choice, long answer and 5 point Likert scale questions. The survey questions can be seen in appendix J.3.

Experimental Procedure: The older adults spent time used the application in their own time without the presence of the author and then filled out the evaluation survey online also with the author present.

Results Analysis: To analyse the results of the Likert scale questions and questions that were multi choice, numerical values were assigned to each of the responses (Strongly Agree = 5, Agree = 4, Undecided = 3, Disagree = 2 and Strongly Disagree = 1) the same was done for yes or no questions (Yes = 1 and No = 2) in order to find the average response by the participants by adding the responses together and dividing the the total number of participants.

C.2 Results

Access Method: Some general questions were asked to gauge how the web app was accessed and it was found that all the participants used accessed the web app using a laptop or a computer.

Effectiveness and Usability: The results of the table can be seen at table 3. When analysing the results of the survey viewed in table 3 it was clear that the web application performed well in explaining issues to the older adults and it was made clear to the participants what they had to do to be more secure.

Revisiting the Application: When asked if any of the participants would revisit their analysis results 100% of the participants stated "Yes". 4 out of the 6 participants mentioned the reason they would come back to the analysis was password related "I will try to find out about random passwords". The other responses were based on reviewing the areas where they need to pay more attention.

Feedback and future work: The participants were asked "*Is there anything you feel is missing from this website or analysis?*" 5 out of the 6 responses replied with "*No*" one person out of the 5 said "*Nothing missing. Very helpful having the analysis done*".

The last participant replied to the question with "Website is very professional and user-friendly" however, had 2 comments on the solutions provided "I have concerns about relying completely on 2-factor authorisation e.g. mobile phone stops working" which is a valid point as this is one of the main research questions regarding multi-factor authentication that there is not an elegant and usable method to access your accounts if one of the factors are unavailable. The second comment was "These very strong passwords are impossible to remember, so would need to be secured safely. How can this be done securely and cheaply?" this feedback leads to a future feature that could be added to the web application, where there is an option to generate a secure password, the generator produces 3 random words where the length is longer than 12. For example "*waterbottle-table-octopus*" a password which is 25 characters long yet would be easier to remember and say out loud than a random set of 12 characters, numbers and symbols such as "*vqgh5frrKNZ5*"

D LEGAL, ETHICAL, PROFESSIONAL AND SOCIAL ISSUES

D.1 Summary of Legal Issues

During the 2 user studies and when developing the application, clear attention was given to the handling of information legally as the appropriate actions were taken to securely store anonymised data from the 2 user studies and when anonymising the final dataset. All the information and resources created in this project should be used for educational purposes only. Full copyright laws were paid attention to as all images and information that was not created within the project were provided the appropriate citations. The user studies were conducted in line with the current Covid-19 restrictions at the time.

D.2 Summary of Ethical Issues

An Ethics application was approved by the University of Dundee School of Science and Engineering Ethics Committee. One amendment was later made in order to change the medium of video conferencing due to the older adults from the User Centre being familiar with Zoom and specifically requesting it thus the amendment was also approved.

No passwords or sensitive information was ever passed during the user studies as it was made clear that the participant did not have to answer any questions they did not want to nor feel pressured into supplying a reason when pulling out of the study.

Another ethical concern was the transfer of passwords over HTTP could be intercepted and viewed in plain text thus it was ensured when hosting the web application, the hosting service provided a TLS certificate thus the communication between the

client and server were fully encrypted and even if intercepted the attacker could not read the data.

When generating passwords for the older adult to use, the passwords are **never** saved and refresh every time the analysis is ran thus there is no possible way for the author or a potential adversary to access the suggested passwords even if the original account structure file is compromised.

D.3 Summary of Professional Issues

Throughout this project the British Computing Society Code of Conduct was adhered to. The professional practices such as industry standard tools, languages and frameworks were used in the development of this project and have been presented throughout the report.

D.4 Summary of Social Issues

The older adults were given the appropriate support and accessibility options throughout this project such as offering breaks during user testing, providing alternative methods of information such as reading documents out loud and tried to ensue a WCAG A/AA standard of accessibility plus usability within the web application.

E CRITICAL EVALUATION

I feel the project went really well and fit within the defined the timeline of 6 months. There was high momentum during Semester 1 where the project was defined and a literature review had been conducted were the reports abstract, introduction, related work and research questions section were complete. Also in Semester 1 the first user study was developed and an ethics application was submitted in December 2020.

In semester 2 I feel the motivation and drive was still very much present and high. The first set of user studies took place as soon as they could in order to gather data to start development. Later designs and requirements were created then development of the application. I was out of my comfort zone during all the phases of the project but this was a good thing as it supported me to learn and problem solve. I learned a lot about myself and the academic side of computing research.

Out of the whole experience the only thing I would change was that even though everything fit within the time limit I would prefer if the design phase was shorted by a week in order to start the development phase slightly earlier thus leaving time for another development sprint or allowing more time to work on the final report.

E.1 Project Problems and Difficulties

Due to Covid-19, the government guidelines meant that the interviews could only take place over video conferencing software, thus there was a much smaller number of participants involved in the two user studies. Two people even pulled out of participating due to not wanting to use video conferencing software after showing interest in the project.

F INTERVIEW SCRIP PART 1

F.1 Demographic

(1) What age bracket do you fit into
  (a) 60-69
  (b) 70-79
  (c) 80-89
  (d) 90-99
  (e) 100+
(2) What sex would you classify yourself as?
  (a) Male
  (b) Female
  (c) Transgender
  (d) Non-Binary
  (e) Other
  (f) Prefer not to say
(3) What is/was your occupation
(4) How do you personally rate your technological literacy?

F.2 Finding Information Security Advice

(1) How important do you think it is to be secure online?
(2) How do you decide what your online security practices are?
(3) Do you face any challenges implementing online security for your situation?
(4) How do you prefer this type of information being presented to you?

F.3 Day to Day Security

(1) What do you do to keep yourself secure online?
  (a) Why?
(2) Are you worried about your online security?
  (a) Why?
(3) What do you wish was easier regarding online security?

G INTERVIEW SCRIP PART 2

For the following section I will ask you questions about your account ecosystems.

For each item you introduce you will give it a nickname such as facebook1, password2 or emailOL this is so you can converve your privacy and not disclose any of your passwords.

Please **DO NOT** share the any sensitive information such as Passwords and Pin codes.

If there are similar accounts, we can duplicate an account We can go back to questions you have already answered if you want.

G.1 Devices

(1) What devices do you use to access the internet?
  (a) For each device give it a nickname. (Examples: Laptop1, WorkPhone2, AppleWatch1)
  (b) What are the login methods and things you need to access this account?
    (i) For each method give a nickname for each entity needed or refer to the nickname that entity was given if already mentioned in the interview.
    (ii) Is this method a recovery method for this account?

(c) Can you view messages and notifications on this device when it is locked?
(d) Are there any comments you have on this device you would like to share?

Repeat 1a-d for every Device

G.2 Password Managers

(1) Do you use password managers to access any of your accounts?
(a) For each password manager give it a nickname. (Examples: PM1, Manager1, LP23)
(b) What are the login methods and things you need to access this password manager?
(i) For each method give a nickname for each entity needed or refer to the nickname that entity was given if already mentioned in the interview.
(ii) Is this method a recovery method for this account?
(c) Do you have any open sessions (being logged in permanently) with this account currently?
(i) For each open session on that account assign a nickname for each entity or refer to the nickname that entity was given if already mentioned.
(d) Are there any comments you have on this password manager you would like to share?

Repeat 1a-d for every account in this category

G.3 Emails

(1) What email addresses do you have access too?
(a) For each password manager give it a nickname. (Examples: OL1, Email76, GM23)
(b) What are the login methods and things you need to access this email?
(i) For each method give a nickname for each entity needed or refer to the nickname that entity was given if already mentioned in the interview.
(ii) Is this method a recovery method for this account?
(c) Do you have any open sessions (being logged in permanently) with this account currently?
(i) For each open session on that account assign a nickname for each entity or refer to the nickname that entity was given if already mentioned.
(d) Are there any comments you have on this email you would like to share?

Repeat 1a-d for every account in this category

G.4 Social Media

(1) What social media accounts do you use to stay connected?
(a) For each social media account give it a nickname. (Examples: SM1, SN23, SOCIAL34)
(b) What are the login methods and things you need to access this account?
(i) For each method give a nickname for each entity needed or refer to the nickname that entity was given if already mentioned in the interview.
(ii) Is this method a recovery method for this account?
(c) Do you have any open sessions (being logged in permanently) with this account currently?
(i) For each open session on that account assign a nickname for each entity or refer to the nickname that entity was given if already mentioned.
(d) Are there any comments you have on this account you would like to share?

Repeat 1a-d for every account in this category

G.5 Finance

(1) What accounts do you have to access your online finances?
(a) For each account give it a nickname. (Examples: B1, BANK23, PAYPL34)
(b) What are the login methods and things you need to access this account?
(i) For each method give a nickname for each entity needed or refer to the nickname that entity was given if already mentioned in the interview.
(ii) Is this method a recovery method for this account?
(c) Do you have any open sessions (being logged in permanently) with this account currently?
(i) For each open session on that account assign a nickname for each entity or refer to the nickname that entity was given if already mentioned.
(d) Are there any comments you have on this account you would like to share?

Repeat 1a-d for every account in this category

G.6 Shopping

(1) What accounts do you use for online shopping?
(a) For each account give it a nickname. (Examples: AZ1, SHOP23, BH34)
(b) What are the login methods and things you need to access this account?
(i) For each method give a nickname for each entity needed or refer to the nickname that entity was given if already mentioned in the interview.
(ii) Is this method a recovery method for this account?
(c) Do you have any open sessions (being logged in permanently) with this account currently?
(i) For each open session on that account assign a nickname for each entity or refer to the nickname that entity was given if already mentioned.
(d) Are there any comments you have on this account you would like to share?

Repeat 1a-d for every account in this category

G.7 Entertainment

(1) What accounts do you use for entertainment?
(a) For each account give it a nickname. (Examples: NT1, DP23, PM34)
(b) What are the login methods and things you need to access this account?

(i) For each method give a nickname for each entity needed or refer to the nickname that entity was given if already mentioned in the interview.
(ii) Is this method a recovery method for this account?
(c) Do you have any open sessions (being logged in permanently) with this account currently?
(i) For each open session on that account assign a nickname for each entity or refer to the nickname that entity was given if already mentioned.
(d) Are there any comments you have on this account you would like to share?

Repeat 1a-d for every account in this category

G.8 Gaming

(1) What accounts do you use for gaming?
(a) For each account give it a nickname. (Examples: CS1, GG23, GM34)
(b) What are the login methods and things you need to access this account?
(i) For each method give a nickname for each entity needed or refer to the nickname that entity was given if already mentioned in the interview.
(ii) Is this method a recovery method for this account?
(c) Do you have any open sessions (being logged in permanently) with this account currently?
(i) For each open session on that account assign a nickname for each entity or refer to the nickname that entity was given if already mentioned.
(d) Are there any comments you have on this account you would like to share?

Repeat 1a-d for every account in this category

G.9 Other

(1) Are there any more accounts or items you feel we have missed?
(a) For each account give it a nickname. (Examples: O1 NP23, OB34)
(b) What are the login methods and things you need to access this account?
(i) For each method give a nickname for each entity needed or refer to the nickname that entity was given if already mentioned in the interview.
(ii) Is this method a recovery method for this account?
(c) Do you have any open sessions (being logged in permanently) with this account currently?
(i) For each open session on that account assign a nickname for each entity or refer to the nickname that entity was given if already mentioned.
(d) Are there any comments you have on this account you would like to share?

Repeat 1a-d for every account in this category

G.10 Password Summary

(1) Look over the passwords you mentioned
(a) How secure do you think your password is:
(i) Strong = A password created by a password manager
(ii) Average = A password **YOU** made yourself that **YOU** consider strong
(iii) Weak = A password you made yourself that you consider weak **OR** if they do not fit in the other two categories
(b) What are the login methods and things you need to access this password?
(i) For each method give a nickname for each entity needed or refer to the nickname that entity was given if already mentioned in the interview.
(ii) Is this method a recovery method to access this password?
(c) Are there any comments you have on this password you would like to share?

Repeat 1a-d for every password in this category

H ACCOUNT ACCESS INTERVIEW TOOL

The tool that was used to collect account structure information is available to view and use through the following link: https://github.com/mabraham123/account-access-interview-app

I EVALUATION INTERVIEW SCRIPT

I.1 Checking the participants awareness of their security

(1) What did you think was the most important part of your account ecosystem?
(2) Are you aware of any account security vulnerabilities you may currently have?
(3) Which of your account(s) do you think are the most important to keep secure?
(4) Are you aware of anything you can do currently to improve your account security?

I.2 Reflections

(1) Were there vulnerabilities found within the analysis based on a security practice that you originally thought secure?
(2) Are there any practices you currently do you thought were not secure but disproved by the analysis?

J EVALUATION SURVEY QUESTIONS

J.1 Meta Data Gathering

(1) What did you use to access this website? (Device and Browser)

J.2 Effectiveness of the System

The following questions are answered using a 5 point Likert scale (Strongly Agree, Agree, Undecided, Disagree and Strongly Disagree)

(1) The information was explained clearly
(2) The website was intuitive to use
(3) It is clear to me what my most important account is
(4) It is clear to me what my security issues are
(5) The solutions for each security issue are presented clearly
(6) It is clear to me what i am doing well currently to keep myself secure

(7) I am very likely to act on this information that was provided in the analysis
(8) If I wanted to research more into the analysis that was provided on my own I would know which direction to look.

J.3 General

(1) Do you see yourself revisiting this analysis?
  (a) Yes
  (b) No
  (c) Explain (Optional)
(2) Was there anything in the analysis that surprised you?
(3) Is there anything you feel is missing from this website or analysis?

K ACCOUNT ACCESS GRAPH DATASET

The full dataset of Account Access Graphs modelling personal account ecosystems created by older adults along with their corresponding JSON data files are available using the following link: https://github.com/mabraham123/protecting-older-adults-online-files/tree/main/Older_Adults_Dataset_Account_Access_Graphs

L USER PERSONAS

The user personas can be viewed at the following link: https://github.com/mabraham123/protecting-older-adults-online-files/tree/main/Personas

M SOURCE CODE

The source code is available when following the link: https://github.com/mabraham123/protecting-older-adults-online

N USER MANUAL

The User Manual is available when following this link: https://github.com/mabraham123/protecting-older-adults-online-files/blob/main/User%20Manual/usermanual.md

O MEETING MINUTES

The Meeting Minutes are available when following this link: https://github.com/mabraham123/protecting-older-adults-online-files/tree/main/Meeting%20Minutes

P ETHICS SUBMISSION

The Ethics Submissions are available when following this link: https://github.com/mabraham123/protecting-older-adults-online-files/tree/main/Ethics%20Submissions

Q RAW SURVEY DATA

The raw servery data is available when following this link https://github.com/mabraham123/protecting-older-adults-online-files/tree/main/Raw%20Survey%20Data

R MID-TERM REPORT

The Mid-Term Report is available when following this link: https://github.com/mabraham123/protecting-older-adults-online-files/tree/main/Mid%20Term%20Report

S LOGBOOK

The Logbook is available when following this link: https://github.com/mabraham123/protecting-older-adults-online-files/tree/main/Logbook