# “I’m Doing the Best I Can.”

Abraham, Melvin; Crabb, Michael; Radomirović, Saša

*Published in:*
11th International Workshop in Socio-Technical Aspects in Security and Trust

*DOI:*
10.1007/978-3-031-10183-0_5

*Publication date:*
2021

*Document Version*
Peer reviewed version

# *"I'm Doing the Best I Can."*

## Understanding Technology Literate Older Adults' Account Management Strategies

Melvin Abraham[1], Michael Crabb[2], and Saša Radomirović[3]

[1] University of Glasgow, Glasgow, UK
m.abraham.1@research.gla.ac.uk
[2] University of Dundee, Dundee, UK
m.z.crabb@dundee.ac.uk
[3] Heriot-Watt University, Edinburgh, UK
sasa.radomirovic@hw.ac.uk

**Abstract.** Older adults are becoming more technologically proficient and use the internet to participate actively in society. However, current best security practices can be seen as unusable by this population group as these practices do not consider the needs of an older adult.
**Aim.** We aim to develop a better understanding of digitally literate, older adults' online account management strategies and the reasons leading to their adoption.
**Method.** We carry out two user studies (n=7, n=5). The first of these gathered information on older adults' account ecosystems and their current online security practice. In the second, we presented security advice to the same group of older adults facilitated by a bespoke web application. We used this to learn more about the reasons behind older adults' security practices by allowing them to reflect on the reported security vulnerabilities in account ecosystems.
**Results.** Our participants are aware of some online security practices, such as not to reuse passwords. Lack of trust in their own memory is a critical factor in their password management and device access control strategies. All consider finance-related accounts as their most important accounts, but few identified the secondary accounts (e.g. emails for account recovery) or devices that provide access to these as very important.
**Conclusions.** Older adults make a conscious choice to implement specific practices based on their understanding of security, their trust in their own abilities and third-parties, and the usability of a given security practice. While they are well-aware of some best security practices, their choices will be different if the best security practice does not work in their personal context.

## 1 Introduction

Older adults (70+) are an underrepresented demographic in cyberspace and can unconsciously be ignored when designing secure cyber-systems [46]. An increasing number of older adults use the internet and smart devices [33]. Some

actively seek to improve their technological literacy through training [1] and university programmes [7]. However, older adults, as a demographic, are also regularly targets of cybercrime [42, 2] and they have traditionally been seen as less technologically literate [6, 16].

For more than a decade a considerable effort has been invested in understanding the strategies used by end-users when securing their online accounts. We call a user's online accounts and the physical and digital means that provide access to them an *account ecosystem*. Keeping a secure account ecosystem is becoming increasingly difficult due to the number of online accounts that each individual owns and the multitude of methods used to secure a growing number of systems. It is unclear whether the problems associated with managing multiple accounts are compounded for older adults due to technology literacy and age-related decline.

In this work, we attempt to understand the methods used by older adults when securing online accounts, and why their chosen strategies are adopted. We carried out semi-structured interviews to gain information regarding online account structures within a group of 7 older adults. We then developed a system that can highlight security issues within an individual's online account graph and used this as a conversation aid to conduct secondary interviews with the same group. We used this second set of interviews to uncover the reasons behind current security practice adoption.

This research contributes an understanding of account security strategies that are used by older adults. The demographic that we include in this work can be classed as digitally literate and yet still at a high risk of being targeted for cyber-attacks. We see this work as developing a niche understanding of the current security strategies that are used by this group which can inform future development of security tools.

## 2 Related Work

Older adults are more at risk of attacks aimed at their online security compared to other age demographics [16]. This increase risk of attack is, in part, due to older adults having better financial stability [27], and also being more trusting towards advice given [25] due to aspects such as social isolation [3]. Older adults are particularly vulnerable to social engineering attacks [3, 17], likely caused by high levels of trust and a low ability to gauge accuracy of advice that is received [44]. The impact of attacks is amplified for older adults as they have fewer digital strategies in place to protect themselves against spam and phishing attacks, as compared to younger adults [17].

Older adults face technical uncertainty when implementing security best practices online [13] and are likely to prioritise security advice based on the availability of advice rather than advice expertise [32]. Being overly trusting and taking information at face value creates challenges in gauging the accuracy of such advice. Following bad security advice can lead to accepting and believing

fake news [26], an increased risk of social engineering [26], and a potentially false sense of security by entrusting others, such as family members [22, 36].

### 2.1 Securing Online Accounts

Many strategies are used to secure accounts including password creation, password management, and additional security tools such as multi-factor authentication. Password based authentication continues to be the dominant authentication method for online accounts.

Guidance exists to assist in creating passwords that are secure for online usage [15, 30]. However, it is recognised that password reuse is a common method used by people when securing their online accounts [8], with this likely due to the challenges associated with remembering multiple complex pieces of information [47]. Password reuse creates an account security vulnerability which an attacker can exploit [8]. When one shared password is discovered for a user through methods such as a password database breach [8], dictionary attack [20] or just guessing, every account that shares the same password is also at risk of compromise [23].

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 that facilitate the use of distinct, strong passwords by assisting with their generation and removing the need to remember them. Despite the clear benefits, adoption rates for password managers with built in password generation features are poor [35, 43]. Adoption is even lower for older adults with suggested reasons for this being a lack of independence, trust and usability [38]. Reasons for not using password managers can include suspicion of the software, and a belief that there is not a current need to adopt this tool [35, 10].

There are many authentication methods that are employed in addition to or instead of standard password authentication. One of the simplest is single sign-on, whereby an account with one service provider is used to authenticate to another service provider. Other authentication methods rely on out-of-band communication, such as the sending of a code to a mobile device the user has access to and is the sole owner of. A related and frequently used authentication method to recover access to an account is by proving ownership of a particular email address. More recent authentication methods employ authenticator apps on smart devices or dedicated authentication devices such as U2F security keys. End-user devices also employ biometric authentication. Finally, two ore more authentication methods that all rely on different authentication principles, such as biometrics, secret information or physical artefacts, can be chained to yield a stronger authentication method. These are known as multi-factor authentication methods. A typical two-factor authentication method is the combination of password authentication with a code sent to a mobile device.

### 2.2 Understanding Links between Accounts

With each account, authentication method or artefact that is added into the security practice of an individual, their account ecosystem grows. This growth can occur, for example, due to an online account's additional requirement for 2-factor authentication. The new authentication method may require both the user's password and a code sent to the user's phone. A look at the bigger picture outside the blinders of individual accounts brings to light critical security issues and lack of best practices which cannot be identified when accounts are considered individually [19].

Account access graphs [19] are a convenient tool to represent an account ecosystem and examine it for security issues. An account access graph is an edge-colored, directed graph whose edges represent a "gives access to" relation between the graph's nodes which represent accounts, devices, sensitive information, or physical objects. Equally coloured edges pointing to the same target node indicate that access to all source nodes is necessary to gain access to the target node. Edges of different colours thus represent alternative access methods.

As with all demographic groups, older adults are increasing the length of time that they use technology for, and the types of services that they engage with online [33]. This increase bring additional challenges in maintaining secure practices for a growing number of online accounts. In order to understand this area and to develop an insight into the challenges that may be present, we ask *RQ: What are the account management strategies used by older adults, and why are these strategies adopted?*

## 3 Older Adults' Account Ecosystems

Recall that an *account ecosystem* is the collection of a user's online accounts and all the physical and digital means that provide access to the accounts. The typical means to obtain access to an online account are credentials such as (cryptographic) private keys and passwords, physical devices such as smart phones, and other accounts such as email recovery and single sign-on accounts.

In order to understand an older adult's personal account management strategy, we must first elicit information on their account ecosystem. To achieve this, we carried out semi-structured interviews with 7 older adults. Each interview was conducted by the same person to ensure coherence and consistency between all the interviews and each interview lasted between 60–90 minutes. The participant's personal account ecosystem was modelled as an account access graph [19] (see Section 2.2) which we annotated with additional information gathered during the interview.

### 3.1 Study Setup

***Demographic Information:*** We recruited 7 participants, all living in North East Scotland. 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 to the participants of this study as P1, ..., P7.

***Interview Setup:*** The semi-structured interview took place using video conferencing software. 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 throughout the process.

***Interview Script:*** An interview script (see Appendix A) based on a script of Hammann [18] 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 and any interesting points brought up to be explored and elaborated on.

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 participant's 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.

***Procedure:*** This study was reviewed and approved by the University of Dundee's Ethics Committee (*UOD-SSEREC-DoC-UG-2020-004*) before any study sessions were carried out. 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 participant's experiences and views and 2) eliciting the participant's account ecosystem by creating their Account Access Graph.

The interview started by asking questions to gauge demographic information. Participants were then 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.

Once all account information was collected, the participant was asked questions relating to how they go about finding information security advice, with this following the study's 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.

***Analysis Technique:*** 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 the risk of bias. Following guidance from [11], interviews were transcribed and anonymised before analysis. Individual sections of the interviews were then analysed independently using open coding [45] where the following process was used:

1. **Generating Initial Codes:** The lead author transcribed all interviews and subsequently took notes of initial codes. These were then collated and developed into a codebook.
2. **Evaluation of Codes:** The lead and secondary author discussed all codes and developed initial descriptions of each.
3. **Coding of Full Data Set:** The lead author then coded the complete dataset using the updated set of descriptors made in Step (2).
4. **Defining Themes:** The lead and secondary authors reviewed the final coding and identified similarities to create thematic groups. This was carried out as a collaborative session where all codes were examined.

The final outcome of our analysis is a broad understanding of older adults' security practices and not of the codes themselves. As such, inter-rater reliability is not relevant [28].

### 3.2 Results

The number of accounts that our participants reported to have in active use ranged from 6 to 21 with a median and average of 12. This is lower than the average of 16–26 accounts a person was found to have in previous studies [35, 34, 12, 48]. All participants had one or more email accounts, financial accounts and social media accounts, and two or more shopping accounts. All participants used several devices to access their online accounts. Multi-factor authentication was only used when it was mandatory.

Whilst the primary purpose of this first interview was to collect information regarding older adults account ecosystem to analyse and use within the second interview in this study, we also gathered information related to their general mindset regarding online security. A brief summary of this is given below.

**Security practices used by older adults** Older adults use a number of security practices to keep their accounts secure online. Participants discussed their usage of passwords, password management systems, and wariness when using online services.

***Passwords:*** From the participants that were interviewed all of them indicated that they follow what they feel is basic account security hygiene. They stated they did 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 Wariness:*** 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).

**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 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) was 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.

## 4 Engaging Older Adults in Account Security

In order for us to develop a better understanding of the older adults' account security practices while also enabling them to develop an understanding of their security vulnerabilities, we created a web application that provides a personalised account security report. The web application served as a basis for the second interview and highlighted the security vulnerabilities in a participant's account ecosystem which we found in the annotated account access graphs that we created from the first interview.

### 4.1 Security Goal and Threat Model

The security goal that our analysis focuses on is to prevent unauthorised access to our participants' online accounts. The account graphs that we elicited in the first interview modeled all possibilities to access the participant's online accounts under the assumption that they contain all relevant information. This assumption may not be true, as participants could have withheld some information or our systematic elicitation could have missed an access path.

In view of the security goal and our participants' demographic, the main threat actors to our participants' account security are online (remote) adversaries and (local) thieves, but not burglars who we assume to be interested in other valuables than accounts.

We consider threats arising from online password compromise and device theft or inadvertent loss. We do not consider threats arising from online scams, such as phishing emails, direct account compromise from attacks on the service provider, compromise due to application vulnerabilities, such as insecure password managers, and we do not consider threats that would arise from eavesdropping, such as shoulder-surfing attacks.

Specifically for password secrecy, the main relevant threats are offline password guessing attacks and credential stuffing attacks.

### 4.2 Assessment of Vulnerabilities

To assess the participants' online account security, we studied all access paths to their accounts in the elicited account graph under the threat model in Section 4.1. That is, we considered:

- whether access to an account was possible starting from a single credential (password or device) which implies single factor authentication,
- the security of each password with respect to offline password guessing attacks and credential stuffing attacks, and
- the security of each device in case the device is stolen, i.e., whether the device is protected by a PIN or biometric for example.

To assess whether our participants were vulnerable to credential stuffing attacks we looked for reused passwords in the account graph. This relied on the participants correctly reporting that two or more accounts used the same password.

To assess whether our participants were vulnerable to offline password guessing attacks, we used a simple scheme to classify the participants' individual passwords strengths. Our top priority was to prevent the participant from inadvertently revealing any information about their actual passwords other than an estimate of their passwords' strengths. We therefore provided the participants with a very simple decision procedure: (1) A password created by a password manager is strong. (2) A password that the participant generated themselves and considered to be strong is of average strength. (3) If neither (1) nor (2) apply, then the password is weak.

Our simple classification of the participant's password strength is based on the following reasoning.

1. A password generated by a password manager is very likely to provide much stronger protection against guessing attacks than a human generated password of the same length.
   To differentiate between these two cases, we consider a password generated by a password manager to be strong and a human generated password to be at most of average strength.
2. A password that a participant thinks is weak, is very likely weak.
   Thus passwords classified by the participant as weak are considered to be weak and otherwise considered to be of average strength.

We discuss the limitations of this approach in Section 7.1.

### 4.3 Reporting on the Analysis of the Account Ecosystem

We sorted our findings of each older adult's account ecosystem into three categories: *Critical Issues*, *Achieving Best Practices* and *Current Successes*. These categories were chosen to motivate the participants to take on the given security recommendations. The first two categories are used to prioritize the recommendations. The positive examples in the third category are intended to both confirm good practices and to provide the participant with confidence that they are capable of being secure. The three categories contained the following tests.

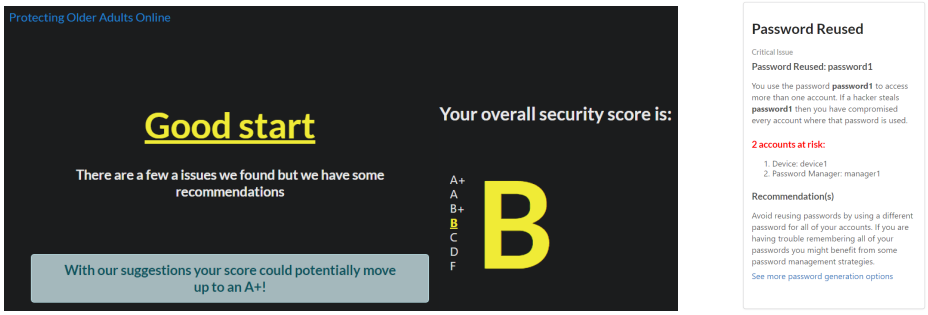


**Fig. 1.** Two web app pages. Initial page showing security grade (left) and a page highlighting a reused password issue (right).

**Critical Issues.** This category concerns vulnerabilities that compromise the older adult's account security and should be fixed as soon as possible. We looked for and classified three types of issues as critical: reused passwords, weak passwords (as self-reported by the user) and devices that give access to an account but are themselves not protected by a password, PIN code, or biometric authentication method.

**Achieving Best Practices.** This category deals with vulnerabilities that should be addressed only after any critical issues are removed. Our best practice tests covered the following criteria: The use of password managers, use of multi-factor authentication, and password strength as reported by the user. Passwords are reported on in this category instead of the critical issues category when the participant considers them to be long and strong, but the password was generated by the participant instead of a random password generator.

**Current Successes.** This category highlights good practices the user is already following but may not be aware of. These results are used to motivate the user by validating their efforts in being secure. The tests for this category are the union of all the tests of the previous two categories. We report in this category the favourable test outcomes. For example, the older adult's use of a password manager or strong passwords would be acknowledged here.

### 4.4 Displaying Security Information

Security information is presented to participants using several techniques. First, a participant is presented with a holistic letter grade in order to contextualise the effectiveness of their current security practices as shown in Figure 1. The letter grade is computed as a sum of scores. Scores were given for

- The percentage of reused passwords
- The number of accounts not employing multi-factor authentication

– Use of a "password manager" (can be a paper notebook)
– The percentage of passwords classified as average strength as discussed in Section 4.2
– The percentage of passwords classified as weak strength
– The percentage of devices that are protected by a PIN, password, or biometric

Second, on separate pages specific issues and information are brought to the participant's attention. An explanation is given what each issue is, which accounts are affected and a usable solution of how to fix the vulnerability is provided as seen in Figure 1 on the right.

The detailed security information was split into the three categories described in Section 4.3. Within each of the categories, and in line with best practice advice [9], the order of displaying the information was based on priority, the most important issues were displayed to the user first. As shown in Figure 1 on the example of reused passwords, we ensured that a clear heading was created for each issue and that the supporting summary explaining the issue used simple non-technical words [21, 39]. Users were presented with a list of what accounts were specifically at risk due to individual vulnerabilities and the display of information concluded with a short concise section for recommendations.

## 5 Older Adults' Awareness of Security Risks

The purpose of our second user study was to improve our understanding of the reasons behind older adults' account management practices. We used semi-structured interviews, combined with a guided walk-through of our security analysis, described in Section 4, as a method to allow participants to discuss their own account security setups. This allowed participants to first demonstrate their own awareness of security risks in their setups and then to reflect on our analysis of their security ecosystems and the impacts that it may have.

### 5.1 Study Setup

***Demographic Information:*** All 7 of the original participants were contacted again. Due to the sensitive nature of the account ecosystem information, each account ecosystem could only be discussed with the participant that it belongs to. Everyone other than P3 and P6 from the previous user study decided to take part in the evaluation thus all the participants will be referred to with the same identifiers.

***Interview Script*:** An interview script (see Appendix B) was developed and used to maintain consistency and coherence between the interviews. The script was designed for a semi-structured interview to allow for conversations to flow naturally allowing any points or views that were brought up to be explored and elaborated on. Interviews took place using video conferencing software.

***Account Security Analysis:*** The previously described web application reporting on the results of the security analysis was shared with participants

during the study. The interviewer shared their screen with participants in order to provide a soft onboarding experience and to guide participants through the different options that were available in the application. 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.

***Procedure:*** This study was reviewed and approved by the University of Dundee's Ethics Committee (*UOD-SSEREC-DoC-UG-2020-004*) before any study sessions were carried out. The study took 20 minutes of the participants' time. At the start of the study each participant was asked questions to record awareness of their own security before seeing their results of the account security analysis. Once these questions were answered the web application was shown to the participants. After the participants had time to view and understand the results of the analysis, the second 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.

***Analysis Technique:*** We used a similar analysis technique to that used in the first study of this paper. All sessions were transcribed, anonymised, and annotated before analysis.

### 5.2 Results

Our analysis technique applied a deductive approach where we intended to focus on highlighting data that would specifically assist in answering our research question. We report on the perceptions that older adults have regarding their online accounts, their awareness of current security vulnerabilities, and their awareness of how their security practice can be improved.

**Perceptions of the most important and secure accounts within account ecosystems.** When classifying which accounts are the most important our participants discussed two factors that they consider. Firstly, which account contains the most valuable data and information and secondly which accounts are the most connected within their 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 a 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.

By our own assessment of participants' account access graphs, each of the participants' primary email account should be considered to be among the most important accounts. For a majority of the participants their email account recovers access to at least one financial account. For all participants it recovers

access to most of the accounts they mentioned during the first interview and in particular to several shopping accounts.

**Awarenesses of current security vulnerabilities.** P2, P4 and P7 expected their potential vulnerabilities to be 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 stated they were not aware of any security vulnerabilities that were 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 because 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 their non digital password management strategy of writing passwords down in a notebook thus avoiding password reuse and being able to choose stronger passwords as they were not relying on memory to use them. For P1 seeing their results (no critical issues, some best practice issues) 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*".

**Awareness of what can be done to increase account security.** Prior to seeing their results, P2 and P7 indicated that if they were 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!*". P7's reaction after seeing their analysis was that "*I will definitely have to look into what counts as a strong password in today's standard.*"

Prior to the results of the analysis, 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 results of the analysis brought up the critical issue that P5 reused a financial account password for several shopping accounts, the reply was that *"I'll be changing my* [financial account] *passwords as ... it was a bit silly to use the same password for some of my other accounts too"*.

## 6 Discussion

Our findings contextualise the account management strategies used by older adults and the reasoning behind their adoption. This gives an insight into older

adults' security habits, their mental model of account ecosystem security, and the practices they choose to implement. We discuss the specifics of the strategies that tend to be used by older adults and the goals and reasons behind managing their accounts with such strategies.

The older adults have shown their mindsets and awareness to their own account security throughout the study in this project. It was found that some of the currently advised security practices, such as not to reuse passwords or use long password [15], may not take into account the needs and context of the older adult. The older adults must make their own risk assessments to gauge if the protection they will acquire from a new security practice is worth the effort to implement and alter their mental security model. As found in our study, the usability of the practice, understanding of what the practice is and how it affects their mental model of security and finally the trust that the practice is sound and secure are the fundamental barriers that must be accounted for when the older adult is deciding whether to implement a practice. We discuss our results grouped into these three areas below.

### 6.1 Usability and Risk Assessment

Each of the older adults in their own way was a victim of expectation to use unusable security practices or practices that are not fit for purpose when considering the needs and situations of the older adult.

Each of the strategies and alterations mentioned in the results were products of the participants' own risk assessments. In the case of P4 and P7, the risk of not remembering the correct authentication information for a device and thus losing access was deemed more realistic and relevant than the risk of the device being stolen. The creation of P2's digital unencrypted file containing passwords was due to similar concerns. Their file is shared with children as a form of digital inheritance [29] to act as a method to access online accounts, posthumously, should this be required.

### 6.2 Trust and Reliance on Third Parties

The older adults' views on trusting third parties to protect them are split. There are some who state that the third parties you trust with your sensitive information have a duty to maintain the confidentiality of the information. Others, however, state that the full responsibility and control must remain with themselves. A commonality between the two mindsets is that they only give away information if they trust the third party.

### 6.3 Understanding of Account and Password Security

It was found that all the interviewed older adults implemented a digital or a physical password management strategy. This is a good start, as the older adults were aware of the risks attached to reusing passwords, and some went out of their

way to ensure that each password is unique. However not all of the strategies are secure. We found that more than 70% of the passwords were generated by the older adults themselves, rather than a password manager and are thus potentially not very strong. For example, it was found that one participant's technique to create unique passwords was to create transformations of a base password. This strategy creates a false sense of security, because modification of basic passwords is a common strategy [8]. Once an individual password leaks, an attacker aware of the strategy has a significant advantage in correctly guessing the password for another account. Since the older adults are already not relying on memory to access a password, it would be worthwhile to support them to improve their understanding of how to automatically and securely generate random passwords with tools that their operating systems provide out of the box, such as the Safari web browser in macOS and the Edge web browser in Windows.

Basing security practices on weak memory alone creates other avenues where the older adults could be at risk. It was discovered when analysing the older adults personal ecosystems, that a considerable risk to their online security could originate from physical risks. If an unprotected device were to be stolen from an older adult it could give access to all the accounts within their ecosystem. Indeed we found that some participants did not have protections such as PINs or biometrics enabled on their devices, as mentioned above for P4 and P7. For others, their protection relied solely on their device's password. Thus the information required to unlock a device would also give the attacker access to the older adult's password manager. This was present in the account ecosystem of P3, where the password required to unlock a device is the same password required to access their password manager application. Similarly in the case of P2 where once the attacker bypasses the password for a device (which was referred to as weak in strength by the participant) the attacker would have access to an unprotected file used to manage their passwords.

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. However, another very important account that was identified was the older adults' primary email. Most of the accounts the older adults have are linked to their email account in that it could be used as a recovery method to access these accounts by means of a password reset. Thus it was recommended that the email account should be the account that is the most inconvenient and difficult for an attacker to compromise, by using a very strong password and enabling multi-factor authentication.

### 6.4 Password Generation and Password Management Advice

We advised our participants to let a random password generator produce passwords for them and to write passwords down in a notebook or store them in a password manager. This advice differs from NCSC [30] guidance in that we do not recommend that users generate their own passwords for the reasons stated

in Section 4.2. NIST 800-63-3 [14] defines a "password" as a memorized secret. We do not advocate memorizing passwords. The NCSC [30] also recommends storing passwords in the web browser.

There are three reasons for our advice. First, given the threat of credential stuffing attacks (Section 4.1), different passwords must be used for different accounts. Thus our advice must consider the fact that our participants will need to generate several different passwords. Everyone, not only our participants' demographic, has difficulties memorizing multiple passwords [37].

Second, based on previous password studies (e.g., [4, 24, 41]), we expect people to generate weak passwords. We expect that this is exacerbated by the pressure to generate different passwords for different accounts and the need to generate memorable passwords. Using a random password generator and writing the passwords down or storing them in a password manager solves this problem and is safe under our threat model.

Third, while the NCSC [31] and NIST [15, Section 5] recommend sensible password policies, not every website or password protected system today adheres to these policies. A password manager can generate passwords adhering to various policies, while studies (e.g. [4, 24, 41]) have shown a human would likely generate a weak password.

## 7 Conclusion

The motivation for this paper's study is to support and empower older adults to protect and defend themselves from cyber attacks that could compromise their account security. As a first step towards this goal we have investigated what the account management strategies used by older adults are and why these strategies are adopted.

We conducted two semi-structured interviews with older adults. In the first interview with 7 older adults we captured their account ecosystem and gained insight into their approach to account security. We analyzed their account ecosystems to assess the effectiveness of their security practices. We then created a web application to present the vulnerabilities that were found and to provide guidance to the older adults on how to improve their online security. The web application was presented to 5 of the 7 older adults in the second interview where we gained a better understanding of what our participants perceive as their current risks compared to what their actual risks are.

Our study tackles the narrative that older adults behave insecurely online. We have found that the older adults in our user study tend to be more wary when online, and will research topics extensively before implementing a security practice. They are wary and careful when it comes to being online and trusting websites or clicking on links. We have also found that their perceptions of security were not far from the reality of the situation.

We conclude that a security practice must conform to three key factors for an older adult to successfully deploy it: Usability, Trust, and Understanding. A deficiency in one or more of these can lead to older adults altering the security

practice to work for them. These alterations can be safe such as employing non digital password management by using a notebook to store their passwords in order to avoid password reuse. They can also be risky such as choosing to not password-protect their mobile devices for fear of forgetting the password.

### 7.1 Limitations

In this work, we collected detailed online account security information and discussed this in depth with participants. We acknowledge that our sample size (n = 7, n = 5) is small and lower than local standards for HCI work (Remote Interviews; mean = 16, SD = 6 [5]). However, it is recognised that studies involving representative users (in our case technology literate older adults) will not have a similar number of participants when compared to traditional HCI experiments [40].

All the participants were recruited from the 'Bytes and Blether' group part of the User Centre located at University of Dundee [7]. This is an initiative by the university to teach technological literacy to older adults. Thus all the participants have access to resources and information on using current technology, have an awareness of security and privacy issues, and may have a greater interest in information technology than the general older adults demographic.

As detailed in Section 4.2, we had to rely on the participants' own assessment of their passwords' strengths and provided them with a simple self-assessment procedure. We rated the participants' passwords as weak if the participants themselves considered their password to be weak. We rated a password to be of average strength if the participant considered it to be strong, but the password was not generated by a random password generator and we rated it to be strong only if it was generated by a random password generator. While password leak studies (e.g. [4]) and password composition studies [24, 41] have shown that people tend to generate weak passwords, it is nevertheless plausible that our simple self-assessment procedure misclassified some participants' passwords. For example, it has been previously observed (e.g. [41]) that people misjudge password strength. Two other potential sources of error are the possibility that the self-assessment procedure was misunderstood or that a random password generation tool was used in a manner that produces weaker than expected passwords.

### 7.2 Future Work

There is much work left to do to help older adults to protect themselves when online. Consideration whether an older adult can effectively implement a security practice must be carried out 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. Our web application is a prototype to both help older adults understand the security of their account ecosystem better and enable a conversation with us to understand their needs better. In future work we plan to extend the scope of the web application to include more automated

analysis techniques, consider different threat models and provide advice on a wider range of topics and authentication methods such as single sign-on.

It is worth repeating the account ecosystem interview and personalised security analysis for demographics other than just older adults. This would allow us to understand the needs and context of the users in the specific demographic and to adapt the web application and provided guidance accordingly.


### Acknowledgments

We are grateful to Karen Renaud for her excellent suggestions on how to improve the paper and the anonymous reviewers for the careful reading and helpful comments. We would also like to thank all members of the Bytes and Blether group at the University of Dundee that took part in this work.


## References


1. Age UK: Computer training courses - it training services (August 2020), `https://www.ageuk.org.uk/services/in-your-area/it-training/`, retr. 2021-09-21
2. Age UK: Uncovering the extent of cybercrime across the uk (June 2020), `https://www.ageuk.org.uk/discover/2020/06/cybercrime-uk/`, retrieved 2021-09-21
3. Alves, L.M., Wilson, S.R.: The effects of loneliness on telemarketing fraud vulnerability among older adults. Journal of elder abuse & neglect **20**(1), 63–85 (2008)
4. Bonneau, J.: The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In: IEEE Symposium on Security and Privacy, SP 2012, 21-23 May 2012, San Francisco, California, USA. pp. 538–552. IEEE Computer Society (2012)
5. Caine, K.: Local Standards for Sample Size at CHI, pp. 981–992. Association for Computing Machinery, New York, NY, USA (2016)
6. Carpenter, B.D., Buday, S.: Computer use among older adults in a naturally occurring retirement community. Computers in Human Behavior **23**(6), 3012–3024 (2007)
7. Crabb, M., Menzies, R., Waller, A.: The user centre. In: History of HCI 2020 (2020)
8. Das, A., Bonneau, J., Caesar, M., Borisov, N., Wang, X.: The tangled web of password reuse. In: NDSS. vol. 14, pp. 23–26 (2014)
9. Egelman, S., Cranor, L.F., Hong, J.: You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In: Proc. SIGCHI Conference on Human Factors in Computing Systems. pp. 1065–1074 (2008)
10. Fagan, M., Albayram, Y., Khan, M.M.H., Buck, R.: An investigation into users' considerations towards using password managers. Human-centric Computing and Information Sciences **7**(1), 1–20 (2017)
11. Flick, U.: The SAGE handbook of qualitative data analysis. Sage (2013)
12. Florencio, D., Herley, C.: A large-scale study of web password habits. In: Proc. 16th International Conference on World Wide Web. pp. 657–666 (2007)
13. Frik, A., Nurgalieva, L., Bernd, J., Lee, J., Schaub, F., Egelman, S.: Privacy and security threat models and mitigation strategies of older adults. In: 15th Symp. Usable Privacy and Security (SOUPS 2019). pp. 21–40. USENIX Association (2019)
14. Grassi, P.A., Garcia, M.E., Fenton, J.L.: Digital identity guidelines (2017). NIST Special Publication 800-63-3 (2017).

15. Grassi, P.A., et al.: Digital identity guidelines: Authentication and lifecycle management. NIST Special Publication 800-63B (2017).
16. Grimes, G.A., Hough, M.G., Mazur, E., Signorella, M.L.: Older adults' knowledge of internet hazards. Educational Gerontology **36**(3), 173–192 (2010)
17. Grimes, G.A., Hough, M.G., Signorella, M.L.: Email end users and spam: relations of gender and age group to attitudes and actions. Computers in Human Behavior **23**(1), 318–332 (2007)
18. Hammann, S.: Secure, Private, and Personal: Advancing Digital Identity. Ph.D. Thesis, ETH Zürich (2020)
19. Hammann, S., Radomirović, S., Sasse, R., Basin, D.: User account access graphs. In: Proc. 2019 ACM SIGSAC Conference on Computer and Communications Security. pp. 1405–1422 (2019)
20. Haque, S.T., Wright, M., Scielzo, S.: A study of user password strategy for multiple accounts. In: Proc. third ACM conference on Data and application security and privacy. pp. 173–176 (2013)
21. Harbach, M., Fahl, S., Yakovleva, P., Smith, M.: Sorry, I don't get it: An analysis of warning message texts. In: International Conference on Financial Cryptography and Data Security. pp. 94–111. Springer (2013)
22. Hornung, D., Müller, C., Shklovski, I., Jakobi, T., Wulf, V.: Navigating relationships and boundaries: Concerns around ict-uptake for elderly people. In: Proc. 2017 CHI Conference on Human Factors in Computing Systems. pp. 7057–7069 (2017)
23. Ives, B., Walsh, K.R., Schneider, H.: The domino effect of password reuse. Communications of the ACM **47**(4), 75–78 (2004)
24. Kelley, P.G., Komanduri, S., Mazurek, M.L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L.F., López, J.: Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In: IEEE Symp. Security and Privacy, SP 2012, pp. 523–537. IEEE Computer Society (2012)
25. Knowles, B., Hanson, V.L.: The wisdom of older technology (non)users. Communications of the ACM **61**(3), 72–77 (Feb 2018)
26. Lee, N.M.: Fake news, phishing, and fraud: a call for research on digital media literacy education beyond the classroom. Comm. Education **67**(4), 460–466 (2018)
27. Martin, N., Rice, J.: 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), 1–15 (2013)
28. McDonald, N., Schoenebeck, S., Forte, A.: Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. Proc. ACM on Human-Computer Interaction **3**(CSCW), 1–23 (2019)
29. Moncur, W., Waller, A.: Digital inheritance. In: Proc. RCUK Digital Futures Conference, ACM, Nottingham, UK (2010)
30. National Cyber Security Centre: Improve your online security today, `https://www.ncsc.gov.uk/cyberaware/home`, retrieved 2021-09-21
31. National Cyber Security Centre: Password administration for system owners, `https://www.ncsc.gov.uk/collection/passwords/updating-your-approach`, retrieved 2021-09-21
32. Nicholson, J., Coventry, L., Briggs, P.: "If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults, pp. 1–11. Association for Computing Machinery, New York, NY, USA (2019)
33. OFCOM: Adults' Media Use & Attitudes report 2020/21, `https://www.ofcom.org.uk/research-and-data/media-literacy-research/adults/adults-media-use-and-attitudes`, retrieved 2021-09-21

34. Pearman, S., Thomas, J., Naeini, P.E., Habib, H., Bauer, L., Christin, N., Cranor, L.F., Egelman, S., Forget, A.: Let's go in for a closer look: Observing passwords in their natural habitat. In: Proc. 2017 ACM SIGSAC Conference on Computer and Communications Security. pp. 295–310 (2017)
35. Pearman, S., Zhang, S.A., Bauer, L., Christin, N., Cranor, L.F.: Why people (don't) use password managers effectively. In: 15th Symp. On Usable Privacy and Security (SOUPS 2019). USENIX Association, Santa Clara, CA. pp. 319–338 (2019)
36. Peek, S.T., Luijkx, K.G., Rijnaard, M.D., Nieboer, M.E., van der Voort, C.S., Aarts, S., van Hoof, J., Vrijhoef, H.J., Wouters, E.J.: Older adults' reasons for using technology while aging in place. Gerontology **62**(2), 226–237 (2016)
37. Pilar, D.R., Jaeger, A., Gomes, C.F.A., Stein, L.M.: Passwords usage and human memory limitations: A survey across age and educational background. PLOS ONE **7**(12), 1–7 (12 2012), https://doi.org/10.1371/journal.pone.0051067
38. Ray, H., Wolf, F., Kuber, R., Aviv, A.J.: Why older adults (don't) use password managers. arXiv preprint arXiv:2010.01973 (2020)
39. Redmiles, E.M., Liu, E., Mazurek, M.L.: You want me to do what? A design study of two-factor authentication messages. In: 13th Symp. on Usable Privacy and Security, SOUPS 2017. USENIX Association (2017)
40. Sears, A., Hanson, V.L.: Representing users in accessibility research. ACM Trans. Access. Comput. **4**(2) (Mar 2012)
41. Shay, R., Komanduri, S., Durity, A.L., Huh, P.S., Mazurek, M.L., Segreti, S.M., Ur, B., Bauer, L., Christin, N., Cranor, L.F.: Designing password policies for strength and usability. ACM Trans. Inf. Syst. Secur. **18**(4), 13:1–13:34 (2016)
42. Simons, J.J., Phillips, N.J., Chopra, R., Slaughter, R.K., Wilson, C.S.: Protecting older consumers 2019-2020: A report of the federal trade commission to congress (2020), https://www.ftc.gov/reports/protecting-older-consumers-2019-2020-report-federal-trade-commission, retrieved 2021-09-21
43. Stobert, E., Biddle, R.: A password manager that doesn't remember passwords. In: Proc. 2014 New Security Paradigms Workshop. pp. 39–52 (2014)
44. Tennant, B., Stellefson, M., Dodd, V., Chaney, B., Chaney, D., Paige, S., Alber, J.: ehealth literacy and web 2.0 health information seeking behaviors among baby boomers and older adults. Journal of medical Internet research **17**(3), e70 (2015)
45. Tracy, S.J.: Qualitative research methods: Collecting evidence, crafting analysis, communicating impact. John Wiley & Sons, Oxford, UK (2019)
46. Vroman, K.G., Arthanat, S., Lysack, C.: "Who over 65 is online?" Older adults' dispositions toward information communication technology. Computers in Human Behavior **43**, 156 – 166 (2015)
47. Wang, C., Jan, S.T., Hu, H., Bossart, D., Wang, G.: The next domino to fall: Empirical analysis of user passwords across online services. In: Proc. Eighth ACM Conference on Data and Application Security and Privacy. pp. 196–203 (2018)
48. Wash, R., Rader, E., Berman, R., Wellmer, Z.: Understanding password choices: How frequently entered passwords are re-used across websites. In: Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016). pp. 175–188 (2016)

# A Interview 1 Script

### Demographic

1. What is your age bracket? (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?

**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?

**Day to Day Security**

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

**Account Ecosystem.** I will now ask you questions about your account ecosystems. For each item you introduce you will give it a nickname such as Social1, Password2 or EmailOL. This is so that you can protect your privacy and not disclose any of your passwords. Please *do not* share any sensitive information such as passwords and PINs. We can revisit questions you have answered.

1. What devices do you use to access the internet?
   (a) For each device give it a nickname. (Examples: Laptop1, WorkPhone2)
   (b) What are the login methods and things you need to access it?
      i. 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 (a)–(d) for every Device.
2. Do you use password managers to access any of your accounts?
   (a) Give each password manager a nickname. (Examples: PM1, Manager1)
   (b) What are the login methods and things you need to access it?
      i. 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 password manager?
   (c) Do you have open sessions (logged in permanently) with this password manager?
      i. For each open session 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 (a)–(d) for every password manager.

The sub-questions 2(a)–2(d) are also asked for each of the Questions 3–9, replacing "password manager" by "account".

3. What email addresses do you have access too?
4. What social media accounts do you use to stay connected?
5. What accounts do you have to access your online finances? What social media accounts do you use to stay connected?
6. What accounts do you use for online shopping? What social media accounts do you use to stay connected?
7. What accounts do you use for entertainment? What social media accounts do you use to stay connected?
8. What accounts do you use for gaming? What social media accounts do you use to stay connected?
9. Are there any more accounts or items you feel we have missed? What social media accounts do you use to stay connected?
10. 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* one that does not fit in the other two categories.
    (b) What are the login methods and things you need to access this password?
        i. 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 on this password you would like to share?

    Repeat (a)–(c) for every password in this category.

## B Interview 2 Script

**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 have?
3. Which of your accounts do you think are the most important to keep secure?
4. Are you aware of anything you can do to improve your account security?

**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?