Widely Reused and Shared, Infrequently Updated, and Sometimes Inherited: A Holistic View of PIN Authentication in Digital Lives and Beyond

Hassan Khan
University of Guelph
hassan.khan@uoguelph.ca

Jason Ceci
University of Guelph
jceci@uoguelph.ca

Jonah Stegman
University of Guelph
jstegman@uoguelph.ca

Adam J. Aviv
The George Washington University
aaviv@gwu.edu

Rozita Dara
University of Guelph
drozita@uoguelph.ca

Ravi Kuber
University of Maryland, Baltimore County
rkuber@umbc.edu

ABSTRACT

Personal Identification Numbers (PINs) are widely used as an access control mechanism for digital assets (e.g., smartphones), financial assets (e.g., ATM cards), and physical assets (e.g., locks for garage doors or homes). Using semi-structured interviews (n=35), participants reported on PIN usage for different types of assets, including how users choose, share, inherit, and reuse PINs, as well as behaviour following the compromise of a PIN. We find that memorability is the most important criterion when choosing a PIN, more so than security or concerns of reuse. Updating or changing a PIN is very uncommon, even when a PIN is compromised. Participants reported sharing PINs for one type of asset with acquaintances but inadvertently reused them for other assets, thereby subjecting themselves to potential risks. Participants also reported using PINs originally set by previous homeowners for physical devices (e.g., alarm or keypad door entry systems). While aware of the risks of not updating PINs, this did not always deter participants from using inherited PINs, as they were often missing instructions on how to update them. Given the expected increase in PIN-protected assets (e.g., loyalty cards, smart locks, and web apps), we provide suggestions and future research directions to better support users with multiple digital and non-digital assets and more secure human-device interaction when utilizing PINs.

ACM Reference Format:
Hassan Khan, Jason Ceci, Jonah Stegman, Adam J. Aviv, Rozita Dara, and Ravi Kuber. 2020. Widely Reused and Shared, Infrequently Updated, and Sometimes Inherited: A Holistic View of PIN Authentication in Digital Lives and Beyond. In *Annual Computer Security Applications Conference (ACSAC 2020), December 7–11, 2020, Austin, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3427228.3427240

ACSAC 2020, December 7–11, 2020, Austin, USA

ACM ISBN 978-1-4503-8858-0/20/12…$15.00
https://doi.org/10.1145/3427228.3427240

1 INTRODUCTION

Knowledge-based authentication (e.g., passwords or PINs) is widely used as it is a well-tested technology and simple to administer [39]. However, research suggests that there are persistent challenges with password usability [7] and memorability [16, 20]. Additionally, passwords are too cumbersome to use for protecting certain classes of assets, such as a car or garage door, which limits their utility.

With the proliferation of technology, it is somewhat ironic that passwords "stubbornly survive and reproduce with every new website" [7]. Challenges with passwords can lead to frustration among users. To address these lingering concerns, several mobile and web apps now provide PIN-based authentication as the default option [38]. Microsoft is also planning to remove the password option from the Windows 10 login screen while keeping PIN as one of the login options [35]. Loyalty cards also require PINs to redeem points, and a survey indicates that an average Canadian participates in twelve loyalty programs, which is a 25% increase over four years [32]. Keyless home locks require PINs to authenticate, and their market is forecasted to reach 35 million units by 2027 [21]. As technologies requiring security in the form of PINs become more prevalent, it is critical to understand how people choose and manage PINs, not just for digital and financial assets, but for the wide array of physical assets for which PINs are used.

In studying PIN management, we broadly categorize PINs into three categories of protected assets: digital (e.g., to unlock digital devices or authenticate to mobile and web apps), financial (e.g., ATM cards or banking apps), and physical (e.g., digital keypad based entry systems for garages or homes). Researchers have explored PIN-based authentication for financial assets, notably Bonneau et al. studied chip-and-PIN systems [8], as well as Wang et al. studied the guessability of PINs as derived from leaked password datasets [47].

We argue that a broader analysis of PIN usage needs consideration for several reasons. First, different types of assets may be subject to different types of attacks (e.g., smartphone PINs might be more susceptible to shoulder surfing [14] than PINs used to protect physical assets), and prevalent reuse across these categories may result in undesirable consequences and increased risks. Second, PINs for certain types of assets may be more likely to be shared (e.g., financial vs. digital asset PINs with a family member), and their careless reuse may result in unauthorized usage. Third, physical PINs are more likely to be shared among family members or by

trusted individuals within their network, which leads to interesting issues surrounding selection of PINs.

Prior work has yet to focus deeply on ways to address the broader considerations associated with PIN usage from a user perspective. In this study, we aim to investigate how users create, manage, and share PINs across different types of assets. To this end, we conducted hour-long, semi-structured interviews with 35 participants. We chose a semi-structured methodology to unpack and better understand the themes relating to use of PINs. Our findings include:

- When selecting a PIN, participants were more likely to prioritize memorability of the PIN over security. While participants reported that reusing a PIN was a low factor in selecting a PIN for a given asset, the majority of participants (28/35 or 80%) reported reusing PINs. This reuse was across different asset types and often resulted in PINs for physical devices (e.g., bike lock) moving into the digital world and vice versa.
- Despite more than two-thirds (71%) of our participants describing situations where their PINs were compromised, less than half of those (45%) reported updating their PINs. This can be attributed in part to concerns relating to memorability and usability of PINs.
- PIN update is very uncommon, overall, and when it does occur, it is often due to reasons of security or memorability (26/49 of reported PIN updates). However, for physical assets such as garage doors, a lack of update may be due to the nature of these devices. Six out of nine owners of PIN-protected garage doors reported that they were unable to update their PIN as they did not know how to perform this action, despite desiring to do so.
- Differences between asset types influence the security measures adopted by users. Participants were less worried about compromising their physical PINs compared to digital PINs, as potential attackers breaking into an entity protected by a physical PIN may face criminal prosecution, e.g., breaking and entering, despite the fact that digital or financial PINs can also lead to personal, financial, or criminal harm.

Based on our findings, we propose three areas for further exploration. First, new intervention and strategies for assisting users in selecting and recalling PINs would address many of the observed shortcomings. While password managers are an obvious solution, their usage is mostly focused on different types of accounts. However, current password managers could be augmented to assist these tasks. Second, as PINs become more pervasive, users may become more concerned with the threat of shoulder surfing attacks. To counteract, the research community should focus on developing new tools to assist users in identifying instances of shoulder surfing, and provide guidance on mitigation practices. Finally, given the plethora of PIN usage scenarios, unifying methods for updating PINs, similar to how password changing has mostly stabilized around standard practice, would make a difference in encouraging PIN updates after compromise. Of course, for physical assets, this is not a simple task. Perhaps augmented reality tools could be used to address this gap in the future, to link these physical assists to known documentation.

2 RELATED WORK

In this section, we explore related work in areas including: PIN choices for human-chosen PINs, attacks on PINs, memorability and reusability of PINs, and lifecycle and management of authentication credentials in general. We also compare and contrast our findings for specific topics related to PIN usage with findings for other authentication methods in Section 5.

2.1 Human-Chosen PINs

Users face several choices when choosing their authentication secrets. Selection is often influenced by factors such as memorability of the chosen secret, reuse of an existing secret, usability (including time to authenticate and error rates), and security [7, 11, 41]. Von Zezschwitz et al. [46] have explored users' choices for text-based password composition, while Biddle et al. [5] have summarized research that explores users' choices of graphical passwords. PINs are less complex than text-based passwords [26] and different from graphical passwords since PINs require memorizing digits.

Amitay collected PINs surreptitiously from an iPhone app in the App Store. Their data showed that ten of the most commonly used 4-digit PINs represented 15% of all PINs in use [3]. Furthermore, most of these PINs followed simple patterns of repeating or consecutive digits. In a seminal work, Bonneau et al. [8] explored the user selection preferences for bank card PINs (e.g., chip-and-PIN systems) using survey data and approximated PINs from leaked password data and Amitay's dataset. They found that an attacker who comes into the possession of a lost wallet with a bank card and owner's ID in it has about an 8% chance of guessing the correct PIN due to the widespread use of birthdays for PINs. Wang et al. [47] compared characteristics (guessability, entropy, and distribution) of chosen 4-/6-digit PINs between English and Chinese users. Among other findings, they showed that the top 5-8% most popular PINs account for over 50% of PIN datasets. Markert et al. [33] collected data on 4-/6-digit PINs, also finding high prevalence of popular PINs, and that the benefit of using 6-digit PINs is minimal (or worse) than a 4-digit PIN. Concurrent to this research, Casimiro et al. [10] conducted an MTurk survey to study PIN choices and reuse and confirm our findings. While these studies offer an insight into the prevalent reuse and not-so-secret nature of human PIN choice, our research extends prior work by examining users' motivations behind their choices.

2.2 Attacks on PINs and Defences

A range of studies have focused on the development and evaluation of novel interaction techniques to defend against shoulder surfing attacks [12, 13, 15, 31, 45]. Researchers have also explored novel side channel-based attacks on PIN authentication, but these attacks require special equipment or skillful attackers [1, 19, 48]. Since these efforts are only tangentially related to our work, we discuss more related works that study attacks and the recourse of victims.

Aviv et al. [4] and Khan et al. [28], empirically evaluated the success of shoulder surfing attacks on PINs under various conditions. De Luca et al. [14] found that German ATM users reported a low incidence of PIN shielding during ATM use. They also reported a significant influence of factors such as distractions, physical hindrance, trust relationships, and memorability on security in PIN-based ATM use. Harbach et al. [22] conducted an online survey and field study

to understand users' smartphone unlocking behaviour. Of users that use a lock code (including PIN and graphical pattern users) for their smartphones, 65% were not or mostly not concerned about a shoulder surfing attack on their code. Other related work includes the study by Eiband et al. [18], who explored shoulder surfing attacks and defences during normal smartphone usage, without focusing on authentication.

Our work expands the existing body of knowledge by exploring attacks on PINs, the defences that are employed, and the recourse of users when they suspect that the attacks are successful for various digital and non-digital assets.

2.3 Security and Memorability of PINs

In an attempt to encourage users to be more secure in their authentication behaviour, researchers have explored methods to generate and help users memorize secure PINs. Kim and Huh [29] found that using a blacklist policy of restricting around 200 commonly used PINs significantly increases the randomness (as measured using Shannon entropy, not guessability [6]) of PINs without significantly increasing the memorability overhead. Findings from a study by Markert et al. [33] indicate that even small blacklists of disallowed PINs can substantially improve the security (as measured using guessability) of user-chosen PINs against throttled attackers. Schechter and Bonneau [41] proposed two techniques to memorize secure PINs and conducted a study to show that the proposed memorization techniques were effective, thereby reducing the likelihood of writing down the new PIN. Stanekova and Stanek [43] and Huh et al. [25] also explored effective methods to generate and memorize PINs. Our work explores memorability and usage issues surrounding PINs without exploring users' memorization strategies, and our findings provide further motivation for the development of effective PIN memorization techniques.

Renaud and Volkamer [40] conducted an online study to evaluate two PIN memorization assistance techniques. While they reported no improvements in PIN memorization due to the users not using the memorization aids, they reported on the strategies people adopted for PIN memorization and whether participants wrote down their PINs. They also identified reasons why participants updated their PINs. However, they did not specify the rate at which different PIN changes occurred and for what reason. We conduct a more holistic and broader investigation of these phenomena. We categorize and quantify the reasons why participants change PINs and report on instances when participants chose not to change their PINs after PIN compromise for different asset categories.

2.4 Lifecycle of Authentication Credentials

Although the lifecycle and management of PINs have not been subjects of much research (either in digital or non-digital contexts), researchers have explored these topics for passwords. Stobert and Biddle [44] investigated how users managed their passwords through a series of interviews. They reported that users ration their efforts to protect their accounts best, and many users reuse passwords as well as adjust them for different accounts. They also found that people were willing to put more effort into the management of accounts with higher perceived importance (i.e., bank account passwords). Hayashi and Hong [23] conducted a two-week diary study to examine password usage of 20 users. They collected data on the frequency and location of password use, and the use of password aids. Based on their findings, they provide suggestions to improve the password authentication experiences of users.

As PIN-based authentication increasingly becomes one of the default authentication options for digital, physical, and financial assets, it is important to understand PIN lifecycle and management across different assets. Our study is the first of its kind to report a holistic view of the lifecycle and management of PINs, thereby highlighting interrelationships across PINs for different types of assets.

3 STUDY DESIGN AND METHODOLOGY

Design. The aim of our study is to better understand how individuals use PINs across a variety of assets. However, there are several challenges to such holistic explorations. First, users may not be attentive to how their PIN management behaviour varies across different assets. Therefore, we chose to conduct semi-structured interviews, which allowed participants to speak openly about their PIN management experiences. This format also provides us with quantitative data, as well as enabled us to ask clarifying and follow-up questions in cases where more detail is needed for qualitative analysis.

Second, collecting user-selected PINs, as used to access a wide range of assets, can quickly become impractical due to the many-to-many mapping between PINs that users employ and the different asset categories. Such a study, while valuable, would be incredibly time consuming and perhaps an error-prone task. Using semi-structured interviews allows us to perform exploratory analysis on the topic with respect to the types of assets protected by PINs and to investigate usage strategies. The findings would provide a greater awareness of exact PINs used in each asset class.

In developing our survey instrument, we initially conducted a pilot study (n = 4) with participants from the first author's department. These participants were invited to a lab where they undertook a structured survey containing questions related to their demographics, their self-reported proficiency with technology and computer security, and whom they lived with (see Appendix A.1 for details). We then asked participants to enumerate all the PINs that they use, and then for each PIN, we inquired about selection (when and how they went about choosing it), resources it protects and the perceived sensitivity of each resource. We then asked about the frequency of PIN entry, others whom they shared that PIN with, and the perceived trust in those individuals. We also asked about any attacks that had been encountered and their recourse. Finally, we asked participants questions applicable to all categories, including sharing across categories, and PIN management after they moved on from a relationship where they had shared a PIN with another individual.

During the pilot, participants had to respond to the same set of questions for up to seven PINs. As a result, they found the survey instrument to be cumbersome, as some of the questions felt unnecessarily repetitive. We addressed this by redesigning our survey across four sections: a section that contained questions that were independent of any asset category or were pertaining to all asset categories; and three sections that contained the same set of questions for each of the three asset categories. This enabled us to

Table 1: Participants' demographics (*UD = Undisclosed)

n = 35							
Gender							
Female				*Male*			
17				18			
Age (in years)							
18–25	*26–30*	*31–35*	*36–40*	*41–45*	*46–50*	*50+*	
8	4	5	6	6	1	5	
Annual Household Income (× $1000)							
>$15	*$15–29*	*$30–49*	*$50–74*	*$75-99*	*$100–150*	*>$150*	*UD**
2	2	3	4	5	10	2	7
Highest Education Level							
High School			*Undergraduate*			*Graduate*	
17			6			12	
Self Reported Proficiency in Technology							
Basic			*Intermediate*			*Advanced*	
6			18			11	
Self Reported Proficiency in Security							
Basic			*Intermediate*			*Advanced*	
19			9			7	

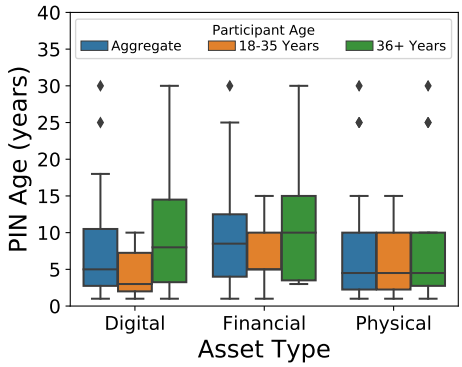

Figure 1: Boxplot of age of oldest PIN currently in use.

Table 2: Statistics of 231 assets that were PIN-protected

Asset	*Total*	*Mean*	*Median*	*Min*	*Max*
Digital	94	2.7	2	0	7
Financial	84	2.4	2	1	7
Physical	53	1.5	2	0	4

collect qualitative data effectively for each PIN category without fatiguing the participants.

From the pilot study, we also noted that users were using multiple PINs in each category (e.g., multiple PINs for multiple banking cards). In the updated survey, while we collected information on how many PINs participants used for each category and across how many assets, we asked participants to respond to our category-specific questions (i.e., PIN choice sharing, reuse, and security-related aspects) for the most used PIN in each category. While this design choice may have resulted in losing some valuable information, it also supported our objective of collecting high-quality data without losing participants' interest due to unnecessary repetition.

The redesigned survey was conducted with a new group of pilot participants (n = 4). All participants completed the surveys within an hour, a more acceptable time frame. The researchers examined the data and found that the categorization of questions across different categories provided more meaningful insights into participants' behaviour regarding the PIN lifecycle. Therefore, this improved survey was employed for our main study (also provided in Appendix A.2).

Methodology. We received approval from our ethics board for this study. We recruited participants from a local classified ad portal, flyers posted around the local area, and word-of-mouth advertising. Participants were offered $25 for their participation in an hour-long study conducted on campus at the University of Guelph. They were informed prior to participating in the interview, that they must not reveal their actual PINs to the researchers.

Before the interview, we described digital asset PINs as the PINs that are used to unlock digital devices or authenticate to mobile and web apps. Digital assets enumerated to participants included smartphones, laptops, personal computers, online accounts, voicemail, gaming consoles, apps, smart watches, thermostats, and other smart home devices. While PINs to digital home locks or banking web or mobile apps could be classified as digital PINs, we asked participants to categorize those as physical or financial PINs, respectively. Financial asset PINs were described as the PINs that controlled access to financial assets, including ATM cards, loyalty cards, and banking websites or apps. Physical asset PINs were described as the PINs that controlled access to physical assets, including electronic home locks, home security systems, garage door openers, cars, and bike or gym locks.

During the semi-structured interview, the researcher first asked about the number of PINs participants used and the assets protected by these PINs. The researcher also reminded participants about several assets that could be PIN protected to ensure that participants did not forget any PINs. The researcher then explained each of the three categories of PINs, and provided examples of assets for each category. The researcher then asked category-specific and category-independent semi-structured interview questions.

Table 1 provides the demographic information of 35 participants and shows their diversity in terms of age, socio-economic group, education, and level of technology awareness.

4 RESULTS

We now present our findings. For test statistics, a Pearson's Chi-Squared test was used to compare categorical data, and a Kruskal-Wallis one-way analysis of variance was used to compare Likert scale responses between asset groups [30]. For all tests, a $p < 0.05$ critical value was used for statistical significance. For multiple comparisons of the same data category, we applied Bonferroni correction to p-values and set the significance cut-off at α/n, where n is the number of multiple comparisons [24]. When reporting quotes from participants to represent a theme, we identify the number of participants who expressed that code and provide a representative quote.

Table 3: Reported PIN entry frequency across asset classes.

Frequency	*Digital*	*Financial*	*Physical*
Multiple times/day	21/32 (66%)	3/34 (9%)	10/25 (40%)
Daily	9/32 (28%)	11/34 (32%)	2/25 (8%)
Multiple times/week	—	10/34 (29%)	9/25 (36%)
Weekly	2/32 (6%)	5/34 (15%)	2/25 (8%)
Multiple times/month	—	1/34 (3%)	1/25 (4%)
Monthly	—	4/34 (12%)	1/25 (4%)

Table 4: Reported reasons for 49 PIN updates

Reason for update	*Digital n=22*	*Financial n=18*	*Physical n=9*
Security (preventive)	5	7	3
Security (post-compromise)	3	5	1
Easy to remember	1	4	2
Forgot the PIN	3	1	1
Policy requirement	2	0	0
Impulse	1	1	0
Asset upgrade	7	–	2

4.1 PIN Usage

In total, 140 PINs were reportedly being used by our participants, and per participant, the average number of PINs in use is 4, with a minimum of 1 and a maximum of 15. These PINs are used to control access to 231 assets. As presented in Table 2, 94 (41%) assets are digital, 84 (36%) are financial, and 53 (23%) are physical.

Among the digital assets, participants primarily reported PINs for securing their smartphones, voicemail accounts, and laptops/PCs (32, 22, and 17 digital assets, respectively). For financial assets, participants reported using PINs for banking (debit or credit cards) and other loyalty cards (66 and 16 financial assets, respectively). Among physical assets, participants reported using PINs for keypad entry systems for home (or security systems), garage doors, and dial locks for bikes/gym lockers (17, 19, and 11, respectively).

Participants were asked to rate how important the *security of their assets* is to them on a scale of 1–5 (5 being the most important) for each of the asset types. The median response was 5 all asset types. The mean responses were 4.31, 4.71 and 4.23 for digital, financial and physical assets, respectively. A Kruskal-Wallis test indicated no significant differences between asset groups for the security rating ($H(2) = 4.98, p = 0.08$).

The self-reported daily usage of PINs across each category is provided in Table 3. Participants authenticated to their digital assets more frequently than financial or physical assets, 30/32 (94%) "Daily" or "Multiple times a day" vs. 14/34 (41%) and 12/25 (48%, respectively. While more participants were using their PIN-protected financial assets (e.g., bank cards) daily, they reported using more usable methods of payment, such as NFC-based tap-to-pay.

We asked participants to report the current PIN that they have been using for the longest period of time within each category. Figure 1 shows the responses from all participants as well as responses grouped into two age groups—18–35 years (n = 16) and 36+ years (n = 19). For all participants, the median age of PINs for digital, financial, and physical assets was 5, 8.5, and 4.5 years, respectively. Six participants reported never changing a PIN across any category since configuring those. As the sampled PIN ages were not distributed normally, a non-parametric Kruskal-Wallis one-way analysis of variance test was used to compare PIN ages between groups. However, this test provided no evidence to suggest that PIN age varied significantly between asset types ($H(2) = 2.94, p = 0.23$).

4.2 PIN Choices

We investigate the factors that motivate PIN choices by asking participants to rank the importance of four criteria when they are choosing PINs: security, memorability, usability, and reusability. The normalized score (rescaled to have values between 0 and 1) from the participants is plotted in Figure 2. The ranking was normalized for better comparisons between PIN choices of different asset types.

Figure 2 shows that memorability is the most important factor for participants when they are choosing PINs across different asset types. Security and usability (defined as "ease to enter the PIN" for our participants to differentiate from memorability) were the next most important factors for the participants. While participants reported reusing PINs (see Section 4.5), they ranked reusability as the least important factor for different asset types. The average ranks (1–4, 1 being most important) for memorability, security, usability, and reusability across assets were 1.52, 2.25, 2.83, and 3.40, respectively. A Kruskal-Wallis test shows a statistically significant difference between the ranks chosen for the four criteria ($H(3) = 130.93, p < 0.01$). Post hoc pair-wise comparisons using Mann-Whitney U tests (Bonferroni corrected) between ranks given by participants for each criterion show statistically significant differences between all six pairs of criteria (all $p < 0.001$).

Interview scripts show that while participants ranked reusability as the least important factor, participants were reusing PINs for reasons of memorability.

> *"Its really annoying to have to remember a new PIN so I change them all to the one I was using. I wouldn't be able to keep track of what PIN is for which card if I didn't make them all the same. I have five cards that have PINs."* (P28)

4.3 PIN Update

For each asset category, we asked participants to recall the last time they updated a PIN. Participants reported 49 incidents of PIN changes (22, 18, and 9 for digital, financial, and physical assets, respectively). The number of reported PIN updates differed significantly between asset groups ($\chi^2(2) = 6.58, p < 0.05$).

Table 4 shows that 9/49 (18%) PIN updates across asset types were due to the compromise of PINs. In Section 4.6, we report our findings that the majority of PIN compromises do not result in a PIN update. Another 15/49 (31%) PIN updates were performed as a preventive security measure. The reasons for the update were similar to the following:

> *"Yes, changed it because felt it was good to change. Because its more secure to change it from time to time."* (P16)

Five of the seven participants who updated PINs of their financial asset did so to change the default PIN that was set by the bank for security reasons.

12/49 (24%) of PIN updates were due to memorability reasons—either motivated by participants' decision to choose easy to remember PINs or as a result of forgetting a PIN.

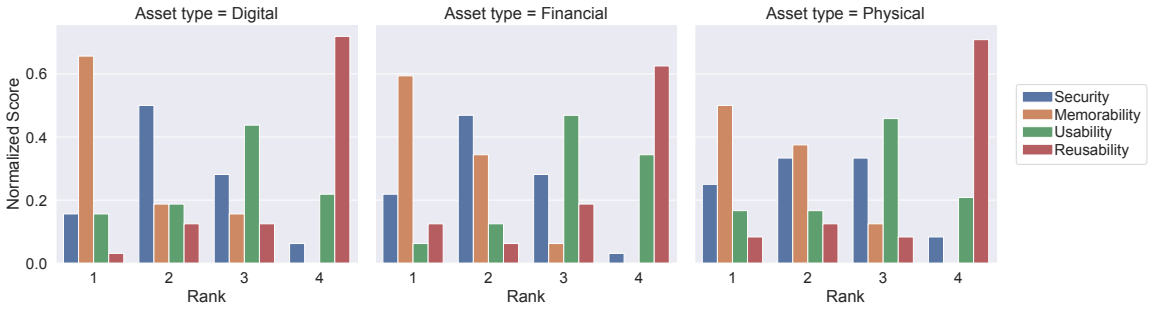

Figure 2: Participants' ranking of security, memorability, usability, and reusability criterion for PINs choices in different categories (lower rank indicates more important choice factor).

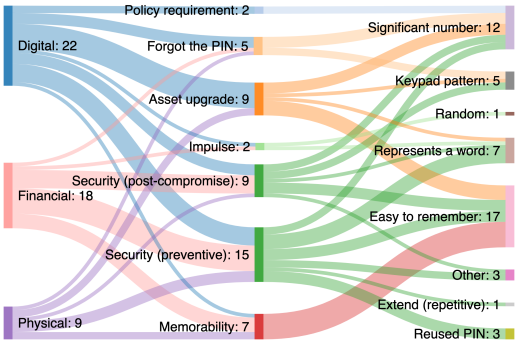

Figure 3: Participants' reasons for PIN update (labels in the center) and strategies for PIN updates (labels on the right).

"I have been using this PIN for various things for 30 years. [I] set my devices to the same PIN when I get them." (P31)

For digital assets, 7/22 (32%) PIN updates were a result of a device (smartphone) upgrade. The reason for PIN updates due to device upgrades are explored below. Other less common reasons included policy requirements and impulsive updates.

Participants were asked to describe the strategy they used to pick the new PIN for each of the PIN update events, and we furthered queried participants about different events that led to PIN updates. The codified responses are reported in Figure 3, which shows that the most popular strategies for selecting a new PIN are choosing an easy to remember number or a significant number, such as a date. Other popular strategies included using numbers that represented a word or using a pattern on the keypad. 17/49 (35%) PIN update strategies were simply reported as an easy to remember PIN. Since patterns or reused PINs are easy to remember, it is not clear how many of these participants were choosing patterns or reusing other PINs. We discovered this confound during our analysis; therefore, for digital assets, we were unable to collect data on what prompted participants to update PINs when they acquired a new device. However, the update strategies show that users employed approaches that result in better memorability (easy to remember or represents a significant number or word). The two cases for physical asset upgrades are reported for situations when participants moved to a new place and updated PINs for digital locks.

It is interesting to note that significant numbers and keypad patterns were popular PIN update strategies despite the reason for update—whether it was security or memorability. Insecure PIN selection strategies were prevalent in high-risk scenarios:

"Yes, suspect my ex-girlfriend had it. I think she saw me enter it in and I changed it after that. I added two digits to the old one to make it a six digit PIN. I added a repeat two digits to the end of the PIN" (P16)

4.4 PIN Sharing

Two factors that possibly influence PIN sharing habits include the type of asset (e.g., home lock vs. smartphone PIN) and co-habitation. For the former, we separately report the sharing habits for different asset types. For the latter, we asked participants whom they lived with: seventeen participants reported living with a spouse, seven with roommates, four with a romantic partner, three with parents, three with siblings, twelve with children, and two by themselves.

The reported statistics for PIN sharing are provided in Table 5. Only a few participants reported not sharing PINs with anyone. For digital assets, only 6/32 (19%) participants did not share their PINs. 21/32 (66%) participants shared PINs for their digital assets with other people that they were in a romantic relationship with. 9 (28%), 5 (16%), and 5 (16%) of the 32 participants shared their digital PINs with children, friends, and siblings, respectively. Four participants reported sharing PINs of their digital assets because they were in circumstances where they felt that they had no other option but to share it temporarily. However, all of them reported not updating PIN after sharing for trust or other reasons:

"I had to share it with my step-child once that I was driving. I thought about changing it but not too keen on changing it since new PINs are a hassle. He visits us once a week only so that is also a factor." (P26)

For financial assets, 7/34 (21%) participants reported not sharing their PINs with anyone. Participants mostly shared their financial asset PINs with their romantic partners (20/34 (59%)) and parents (3/34 (21%)). Only two participants reported sharing with friends to grab lunch or coffee for them. Similar to digital PINs, three participants reported inadvertent sharing of financial PINs and not updating them later.

"I have given it to my son once too to buy something and was concerned if he would try the same on my laptop or smartphone.

Table 5: People that participants reported sharing PINs with.

Shared with	*Digital (n=32)*	*Financial (n=34)*	*Physical (n=27)*
None	6	7	1
Spouse	16	17	13
Children	9	6	8
Parents	3	7	10
Siblings	5	2	5
Girl/Boyfriend	5	3	4
Friends	5	2	9
Helpers	0	0	8

Table 6: Reported reuse of PINs

Have you reused PINs?	
No:	7/35 (20%)
Yes:	28/35 (80%)
Type of reuse	
18/28 across all asset types	
3/28 same asset type only	
4/28 across digital and physical	
3/28 across digital and financial	

Yes, he knows those PINs now [laptop and smartphone PINs—the same as their ATM card] but back then he didn't. Was holding another kid and there was an urgent need to grab water from convenience store." (P24)

As expected, for physical assets, all but one participant shared their PINs with at least one other party. Other than prevalent sharing among friends and family members, 8/27 (30%) participants reported sharing physical PINs with hired helpers (cleaners or pet caretakers). For physical PINs, two cases of inadvertent sharing with strangers were identified. Participants reported not updating the PIN, even after their contact with the third parties had concluded. We discuss the reasons for not updating physical PINs in Section 5.

"Yes, it was shared with the furniture company that went out of business, and nothing was done about it. Never had a problem with the company so there is a trust." (P11)

The self-reported sharing data on PINs from our study shows widespread sharing as well as sharing across different relationship types. Among participants that live with their spouses, all but one (94%) shared their PINs for digital assets. For participants who reported living with a girlfriend/boyfriend, all shared their digital PINs with their partner. This finding is different from Kaye's finding that only a third or fewer participants reported sharing their personal email and Facebook passwords, both primarily with partners and close friends [27]. This difference is expected because Kaye studied sharing habits for specific online services whereas, participants from our study reported sharing habits for assets that are either more likely to be shared (e.g., physical) or assets that are more generic in nature (e.g., smartphones). Our findings are congruent with those of Matthew et al. [34] and Singh et al. [42] that people share passwords with trusted family members.

4.5 PIN Reuse

We asked participants whether they reuse PINs (within the same or across asset categories). Seven (20%) participants reported not

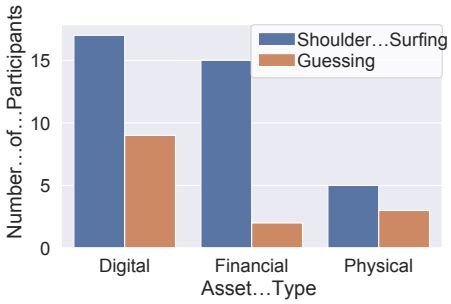

Figure 4: Participants reported attacks on PINs for different asset categories.

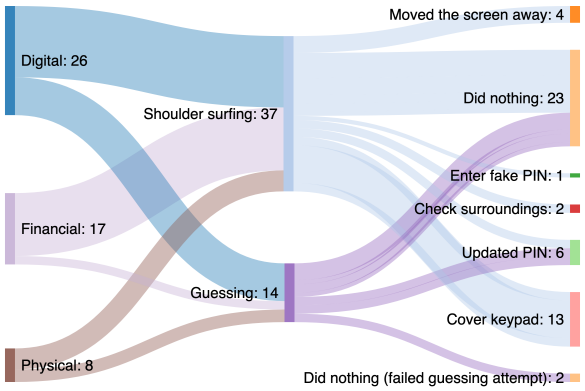

Figure 5: Reported recourse by participants (labels on right) against different attacks (labels in center) on PINs.

reusing PINs at all for security reasons. These seven participants used 1, 2, 3, 5, 5, 6, and 6 PINs in total.

Twenty-eight participants reported reusing PINs. As discussed in Section 4.2, the reported underlying reason for reuse was memorability. Out of these participants, 18 (64%) reported reusing PINs across all categories. Three participants reported reusing PINs within the same category only (e.g., a common PIN for both their phone and tablet). Findings also showed that three participants reported reusing PINs across digital and physical categories, and the same number reported reusing across digital and financial asset categories. Participants' choice to not reuse PINs and create new PINs for some assets was motivated to protect against certain threats.

"[I have] shared PIN-A [(Cell phone, laptop, online account (cell provider))] and PIN-C [(Netflix parental, xBox)] with spouse and PIN-B with kids [(Home, Garage, tab)]." (P25)

During the interviews, several participants demonstrated that they understood the risk of reusing PINs. However, they either considered the reuse to be a secret or a chance worth taking despite the risks involved.

"Well it is the same as my garage and alarm PIN. All financial PINs are the same so I have shared it with my wife, kids, dog walker, and cleaning lady but only my wife knows it's the same PIN for my bank." (P28)

4.6 Attacks on PIN and Recourse

We asked participants to recall the last time a PIN in each asset category may have been subjected to shoulder surfing or guessing attacks, regardless of the outcome of the attacks. Figure 4 shows the distribution of participants who perceive that an attack may have occurred on their PINs of different categories. 25 participants (71%) recall experiencing a shoulder surfing attack or being concerned that a guessing attack had occurred on one or more of their PINs. More participants reported attacks on PINs for digital and financial assets than for physical assets (26 and 17, respectively vs. 8). Similarly, across all asset types, participants reported more shoulder surfing attacks than guessing attacks (37 vs. 14). The number of shoulder surfing and guessing attacks reported both differed significantly between asset types ($\chi^2(2) = 7.74, p < 0.05$ and $\chi^2(2) = 6.84, p < 0.05$, respectively). Significantly more shoulder surfing attacks were reported for financial assets than guessing attacks ($\chi^2(1) = 11.29, p < 0.05$).

We also asked participants regarding the recourse that they took when they were subjected to attacks. Their responses were codified, and a summary of results is presented in Figure 5. For 23 of the potentially successful attacks, participants reported taking no action to prevent shoulder surfing or guessing attacks across different asset categories. The reasons reported for this inaction included trusting the attacker (friend or family member), laziness, or that the attack failed, so they felt action was not required.

> *"Yes, at work some colleagues have seen me enter it. Usually for meetings I have to open my device and enter PIN in front of other people. I am not looking but can imagine that every one who is next to me have seen it. Did not change it and did not protect because it seems like people would think that I do not trust them."* (P35)

Six participants reported updating PINs in response to an attack—four for digital assets and two for financial assets. Note that when participants were asked about why they updated a PIN (for a previous question, see Table 4), more participants reported updating the PIN due to reasons of security. However, that over-reporting is due to compromises through other types of attacks (e.g., online compromise of a PIN-protected financial asset). Other common defences included covering the device screen or moving the screen away from the attacker (similar to the finding of Eiband et al. [18]).

5 DISCUSSION

Our interviews uncovered interesting ways in which different asset categories can impact PIN management and unique security and memorability challenges for PINs. In this section, we discuss these issues. For qualitative analysis, two researchers independently performed thematic analysis to identify themes from participant responses during the semi-structured interview. Identified themes were compared and discussed by reviewers until consensus was reached. This approach is used by other researchers in the field (e.g., Acar et al. [2]).

5.1 PINs in Different Contexts

Our findings show differences between different asset types in how participants share PINs and how PINs are attacked. Participants also reported using different levels of protection for different types of assets. This behaviour was due to different levels of perceived risk to different types of assets and the possible recourse available to the users in case the attacker was successful. For instance, five participants reported being less concerned about physical PINs than digital or financial PINs and had comments similar to the following.

> *"Even if it was access to where the digital devices or money [financial] PINs are [through physical PINs], the risk of breaking a physical PIN is higher for getting caught then the other ones."* (P16)

Similar comments were from two participants who were less concerned about other people learning their financial PINs.

> *"I would be a lot more concerned about someone accessing my phone than my bank account. If a colleague were to look into my phone or laptop I would not have a recourse but if someone were to steal my money that will be a different thing."* (P35)

Two participants also reported caring less about their financial PINs because an attacker with their bank cards will be able to perform transactions without needing the PIN.

> *"Not much [worried about PIN security] and I guess it is a combination of factors. [Bank] card is on me and if someone were to get it they could tap-to-pay or do an online transaction with the number on the back. And in that case there is reimbursement for fraud."* (P35)

Only one participant reported being more concerned about the physical PINs due to their perceived susceptibility to shoulder surfing attacks.

> *"Yes. I am worried someone would watch me enter it. They may have binoculars. I always cover it [hand masking entry]."* (P29)

The comments of participants indicate that with the availability of possible recourse (i.e., police involvement for physical or financial assets), they were less careful about the secrecy of their PINs. Egelman et al. [17] also reported observing this rational behaviour for the use of security features on smartphones and risk perceptions of users. However, while the perception that the attackers are less inclined to trespass on their property may be true, the majority of participants reported reusing their PINs across other categories.

5.2 Attack Susceptibility of PINs

In Section 4.6, we reported our finding that 27/35 (71%) of participants reported attacks on PINs. Another interesting theme that emerged from participants' responses was the high susceptibility of PINs to shoulder surfing attacks. Three participants voiced the concern that it is difficult to enter a PIN without third parties in close proximity learning about it.

> *"My colleagues may know my PIN but not too sure whether it is worth changing it because they will learn the new one too. Mostly this happens when you unintentionally look at someone entering it."* (P24)

This observation was also the reason why two of the participants did not update their PINs after they were compromised.

> *"My kids are not supposed to know it but they must have seen me enter it on my previous phone when I did not have a fingerprint id. [...] I am not too sure who else has knows it or has cared to learn it. I have seen many enter their PINs and patterns before me but never cared for it."* (P33)

During the discussion on guessing attacks, the comments of four participants seemed to indicate that they understood that their PINs were weak and could be easily guessed.

"Didn't ask how he [the perpetrator] got to know but I guess he watched me type it or he may have guessed it since it was simple enough." (P25)

Participants' comments show that they relied on other measures to complement security offered by PINs. These approaches include risk aversion of attackers against attacking financial and physical assets (discussed earlier), aversion of attackers to be recorded in the act, and participants being careful of their assets around attackers:

"For the gym locker PIN, I am worried sometimes because many people are around and I leave my wallet and phone in the bag when going for shower. But there are cameras in some areas so I think people would not try something silly." (P33)

Two participants complained about the PIN entry interface for Netflix Parental lock. These participants complained that on big screens, the Netflix parental lock did not provide them with a way to enter the PIN without giving it away in shared spaces—particularly with the children in the vicinity.

"[...] when my kids ask me to play specific content I've to ask them to leave the room." (P24)

The relative ease with which PINs can be shoulder surfed is known [28]. Our study shows users are aware of this issue, and that it negatively affects trust in PINs as an effective security control. We discuss some remediation in Section 6.

5.3 Memorability Issues

As noted, participants rated memorability as the most important criteria for selecting PINs. This high ranking may be attributed to avoiding potential inconveniences:

"You have to be really quick in restaurants or stores, you can't be guessing and trying to remember it. That's why I keep the same PIN." (P32)

Memorability and ease of entering a known PIN seemed to trump security even for the cases where participants decided to update PINs. Three participants reported that they reluctantly reverted their PINs because of frequent errors.

"Did change after [my girlfriend learned it] because we were living in the same shared space but made so many mistakes that I reverted; entry mistakes from muscle memory" (P27)

Stobert and Biddle [44] found that users found coping mechanisms to live with the difficulties of password authentication. Similarly, PIN users seem to be using strategies to deal with the memorability-related challenges of PIN authentication by compromising security. In Section 6, we discuss some approaches to mitigate these memorability-related challenges.

5.4 PINs and Past Relationships

Park et al. [37] conducted an online survey and found that, among other factors, marriage and co-habitation results in the sharing of online accounts. Our findings are congruent with theirs. Our participants self-reported wide-spread sharing of PINs with their romantic partners.

Nine participants reported sharing their digital PINs with someone that they were in a romantic relationship with in the past. Three of these participants did not change the PIN because they either still trusted that person or they felt there was no need since the other person no longer had access to assets (*"[I] changed it just for more privacy but didn't feel the need to change it."* (P6)). Other participants updated their PINs, although one participant reported that there was no need to do so (*"[Did] nothing as I had the device*" (P3)). One participant reported changing PIN because the other person still cohabited with them.

For financial assets, five participants reported sharing it with people that they were in a relationship in the past, and only two people reported updating it. Note that these participants also reported updating their digital PINs after moving on. Only four participants shared their physical PINs with past relationships, and only one reported updating it. While these PINs were for home or garage access, participants reported not changing those because they still trusted their past partner (*Nothing was done as there was never a problem.* (P13)).

Park et al. [37] identified that individuals are likely to attempt to remove or disable a partner's access to online accounts. We did not find this to be the case for our participants. Unlike with online accounts, participants would need access to assets in addition to the authentication secret (i.e., PINs). However, with the increasing number of online services that accept PINs and the widespread reuse, this may pose a threat to those accounts where PIN has been reused. For such cases, it would be beneficial to consider the guidelines suggested by Obada-Obieh et al. [36] on design improvements of online accounts to support users better when they end account sharing.

5.5 Physical PIN Inheritance and Update

One interesting finding was the "inheritance" of physical PINs that protected garage doors. Nine participants reported moving to another house with a pre-existing PIN set to open the garage door, but only three participants reported updating that PIN while the remaining six kept the PIN set by the previous owner. One participant even reported reusing the inherited PIN for their home lock:

"Garage [PIN was set] by previous owner. [I] used it again for home lock that was installed afterwards" (P27)

Since four of these six participants reported changing the home locks, the lack of the update of garage door PINs cannot be attributed to trust. Instead, this insecure behaviour is due to the lack of knowledge on how to update the PIN:

"No, the garage was setup by previous owner. We did change the key locks and considered updating the garage PIN but there is no information available on it on how to do that." (P34)

This inability to update garage door PIN was also voiced by participants when these PINs were accidentally divulged:

"Once a person who was delivering a package [saw it]. My husband was concerned about it but neither knew how to change it." (P35)

While the instructions on how to update these PINs were missing, two participants did comment that laziness on their part also contributed to the situation, and that they had other resources available.

"[It was shared with the] Garage door repair person when they were here to fix the door. Didn't change it... don't know how to although I can google [search]." (P26)

One participant complained that the previous owner did not share the Master PIN that would allow a PIN update, thereby eliminating their ability to update it. The inability of users to effortlessly update PIN in case of a compromise could potentially result in security issues. In Section 6, we discuss possible remediation strategies.

6 FUTURE RESEARCH DIRECTIONS

PIN choices and management strategies. Our participants reported widely sharing and reusing PINs, and infrequently changing them even after they were compromised. The interviews indicate that the main driving factor behind this risky behaviour was the memorability of PINs. Most participants did not adopt a PIN management strategy by explicitly considering the threat actors. When prompted to choose a PIN, they chose a PIN that they remembered well. Only a few participants considered aspects such as the circles they had to share the PIN with before choosing their PINs. Other factors that need to be considered include the nature of the asset, the susceptibility of attacks on the asset (e.g., shoulder surfing is more of a threat for a smartphone than an ATM PIN), and the type of recourse that is available to participants in the event of a compromise. While these are important considerations, additional research needs to be conducted to understand that a user with an average technology and security proficiency is able to make secure PIN choices given these factors. This will enable researchers to create improvements that actually match user expectations in their everyday lives.

PIN-based authentication is used for six assets on average and recalling the correct PIN for the right asset is problematic for several participants. Existing proposals on the memorability of PINs (discussed in Section 2) do not improve the situation with multiple assets and multiple PINs. A cued recall-based approach that allows a participant to associate pairs of assets and PINs (or corresponding word representation of PINs) may offer mitigation. Digital wallets, for example, enable users to perform secure transactions without entering PINs, but such features are not available for all PINs, particularly physical PINs. Digital apps for smartphones could be designed to help people with such recall issues with features similar to that of a password manager but would enable quick recall for digital, financial, and physical PINs.

Confidence in PINs as a security control. Prior empirical studies report on the susceptibility of PINs to shoulder surfing attacks and users' experiences of such attacks [4, 18, 22, 28]. We also uncovered the limited levels of faith users reported on PINs' resistance to shoulder surfing attacks (see Section 4.6). While simple defences like shielding the keypad while entering a PIN is effective, it is not widely used as it shows the lack of trust to the observers. Improved PIN entry interfaces have been proposed that provide defences against shoulder surfing (discussed in Section 2), but the limited availability of these on smartphones may reduce the efficacy of PINs as an effective security control. We also noted several cases where participants had to inadvertently share their PINs or enter PINs in front of other people. The availability of a short-term device access approach like SnapApp [9] may help users greatly improve the security posture of their digital PINs.

Improved interfaces for PIN update. PIN-based authentication on devices with limited interfaces (e.g., garage doors and digital home locks) introduces unique challenges. Our study shows that users are more likely to continue inherited PINs for such assets due to the lack of clear and readily available instructions on how to update PINs. Furthermore, such assets may require a master PIN to update or reset PINs, and the storage and management of such a PIN further complicates the situation. One participant reported sharing the same PIN with people of different trust levels with (e.g., family vs. pet caretaker) despite the availability of the digital home lock to create different PINs. This was primarily due to the inability of the device to report which PINs were used when.

As the security of an asset is dependent on being able to change the PIN in case of a compromise, there is a need to design a standard way to update and reset PINs on devices with limited interfaces (i.e., only keypad). Alternatively, instructions could be provided on the physical locks to reduce barriers to PIN update on such devices. While the availability of such unifying methods for updating PINs on future devices would make a difference in encouraging PIN updates after compromise, the challenge will remain for millions of devices currently in use. One possible approach is to design augmented reality tools to address this gap by linking these physical assists to known documentation and instructions for updating PINs.

7 LIMITATIONS

Our study has some inherent limitations similar to that of other user studies, which include that many of the findings are based on self-reported data from willing participants. Prior empirical studies of PIN usage on smartphones [22] indicated that participants underreport their daily PIN usage, which may also be the same here. In which case, our results may underestimate the total number of PINs used across asset types, which is compounded by the fact that some categories, such as banking app PINs, could be classified as both digital and financial. In an attempt to mitigate this limitation, we choose to use a semi-structured interview method that included suggestions of assets, to help ensure that participants thought of the diversity of assets where PINs are used.

Additionally, we asked several contextual questions for the most widely used PIN in each category. As a result, our study is limited in scope with regard to the most widely used PINs, but we were able to collect quality responses from participants in a time-constrained lab-based study regarding the PINs that protect the most assets.

We were also limited geographically in our participant pool, which belonged to the Waterloo and Guelph regions in Canada. This is a relatively safe place to work and live (as self-reported by the participants). The safe environment may have implicitly encouraged some of the unsafe practices among our participants for PINs protecting their physical assets. However, we do believe this convenience sample does generalize to many other populations, but not all, and more research would be needed to understand how different populations approach PIN security.

Finally, interviews were conducted by two researchers sequentially, where both researchers used the same semi-structured script of questions. We found that the second researcher elicited more detailed quotes from participants, which are cited more throughout the document; however, data collected by the first researcher are still ecologically valid and were fully used in data analysis.

8 CONCLUSION

We conducted a study with 35 participants to understand how they manage PINs across different assets. Our findings show behaviour that may result in potential compromises due to widespread sharing and reuse of PINs across different asset categories were mainly motivated by reasons of memorability. The memorability concerns also deter users from updating PINs after they are compromised. Participants further reported their lack of confidence in PINs due to their susceptibility to shoulder surfing attacks—a concern that can be mitigated using PIN entry interfaces that resist shoulder surfing. Our study also shows that participants change their PIN management behaviour for different types of assets due to the availability of another recourse in case of a compromise. Finally, we propose further research directions for researchers. With the increasing options to use PINs for purposes of authentication for different types of assets, our findings will help researchers design tools and strategies to improve the security of PIN-protected assets.

ACKNOWLEDGMENTS

We thank Flynn Wolf, Harshvardhan Verma, and Kassidy Marsh for their feedback on the survey and assistance. This material is based upon work supported by NSERC under Grant No. RGPIN-2019-05120 and the National Science Foundation under Grants No. 1845300. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agencies.

REFERENCES

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay cool! understanding thermal attacks on mobile-based user authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM.

[2] Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L Mazurek, and Christian Stransky. 2017. How internet resources might be helping you develop faster but less securely. *IEEE Security & Privacy* 15, 2 (2017), 50–60.

[3] Amitay, Daniel. 2011. Most common iPhone passcodes. http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes. Last accessed June, 2020.

[4] Adam J Aviv, John T Davin, Flynn Wolf, and Ravi Kuber. 2017. Towards baselines for shoulder surfing on mobile authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference*. ACM.

[5] Robert Biddle, Sonia Chiasson, and Paul C Van Oorschot. 2012. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)* 44, 4 (2012), 1–41.

[6] Joseph Bonneau. 2012. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*. IEEE. https://doi.org/10.1109/SP.2012.49

[7] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*. IEEE.

[8] Joseph Bonneau, Sören Preibusch, and Ross Anderson. 2012. A birthday present every eleven wallets? The security of customer-chosen banking PINs. In *International Conference on Financial Cryptography and Data Security*. Springer.

[9] Daniel Buschek, Fabian Hartmann, Emanuel Von Zezschwitz, Alexander De Luca, and Florian Alt. 2016. Snapapp: Reducing authentication overhead with a time-constrained fast unlock option. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*.

[10] Maria Casimiro, Joe Segel, Lewei Li, Yigeng Wang, and Lorrie Faith Cranor. 2020. A Quest for Inspiration: How Users Create and Reuse PINs. In *Adventures in Authentication Workshop*.

[11] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. 2006. A Usability Study and Critique of Two Password Managers.. In *USENIX Security Symposium*.

[12] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.

[13] Alexander De Luca, Katja Hertzschuch, and Heinrich Hussmann. 2010. ColorPIN: securing PIN entry through indirect input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.

[14] Alexander De Luca, Marc Langheinrich, and Heinrich Hussmann. 2010. Towards Understanding ATM Security: A Field Study of Real World ATM Use. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS)*. ACM, Article 16, 10 pages. https://doi.org/10.1145/1837110.1837131

[15] Alexander De Luca, Emanuel Von Zezschwitz, Ngo Dieu Huong Nguyen, Max-Emanuel Maurer, Elisa Rubegni, Marcello Paolo Scipioni, and Marc Langheinrich. 2013. Back-of-device authentication on smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.

[16] Rachna Dhamija and Adrian Perrig. 2000. Deja Vu-A User Study: Using Images for Authentication.. In *USENIX Security Symposium*.

[17] Serge Egelman, Sakshi Jain, Rebecca S Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are you ready to lock?. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. ACM.

[18] Malin Eiband, Mohamed Khamis, Emanuel Von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding shoulder surfing in the wild: Stories from users and observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM.

[19] Denis Foo Kune and Yongdae Kim. 2010. Timing attacks on PIN input devices. In *Proceedings of the 17th ACM Conference on Computer and Communications Security*.

[20] Simson Garfinkel and Heather Richter Lipford. 2014. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust* 5, 2 (2014).

[21] Grand View Research. 2020. Smart Lock Market Demand To Reach 34.9 Million Units By 2027. https://www.grandviewresearch.com/press-release/global-smart-lock-market. Last accessed June, 2020.

[22] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *10th Symposium On Usable Privacy and Security (SOUPS)*.

[23] Eiji Hayashi and Jason Hong. 2011. A diary study of password usage in daily life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM.

[24] Sture Holm. 1979. A simple sequentially rejective multiple test procedure. *Scandinavian Journal of Statistics* (1979), 65–70.

[25] Jun Ho Huh, Hyoungshick Kim, Rakesh B Bobba, Masooda N Bashir, and Konstantin Beznosov. 2015. On the memorability of system-generated pins: Can chunking help?. In *Eleventh Symposium On Usable Privacy and Security (SOUPS)*.

[26] Markus Jakobsson and Debin Liu. 2011. Bootstrapping mobile PINs using passwords. http://www.markus-jakobsson.com/wp-content/uploads/W2SP11-JL.pdf.

[27] Joseph'Jofish' Kaye. 2011. Self-reported password sharing strategies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM.

[28] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2018. Evaluating attack and defense strategies for smartphone pin shoulder surfing. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM.

[29] Hyoungshick Kim and Jun Ho Huh. 2012. PIN selection policies: Are they really effective? *Computers & Security* 31, 4 (2012), 484–496.

[30] William H. Kruskal and W. Allen Wallis. 1952. Use of Ranks in One-Criterion Variance Analysis. *J. Amer. Statist. Assoc.* 47, 260 (1952), 583–621. https://doi.org/10.1080/01621459.1952.10483441 arXiv:https://www.tandfonline.com/doi/pdf/10.1080/01621459.1952.10483441

[31] Luis A Leiva and Alejandro Català. 2014. BoD taps: an improved back-of-device authentication technique on smartphones. In *Proceedings of the 16th International Conference on Human-Computer Interaction with Mobile Devices & Services*.

[32] Macorr Research Blog. 2017. Customer Loyalty Cards in Canada. http://www.macorr.com/blog/?p=342. Last accessed June, 2020.

[33] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. 2020. This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs. In *IEEE Symposium on Security and Privacy (SP '20)*. IEEE, San Francisco, California, USA, 1525–1542.

[34] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. " She'll just grab any device that's closer" A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*.

[35] Microsoft. 2018. Passwordless Strategy. https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/passwordless-strategy. Last accessed June, 2020.

[36] Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. 2020. The Burden of Ending Online Account Sharing. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM.

[37] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. Share and share alike? an exploration of secure behaviors in romantic relationships. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS)*.

[38] PayPal. 2018. Password and PIN Security. https://www.paypal.com/us/webapps/mpp/security/secure-passwords. Last accessed June, 2020.
[39] Karen Renaud and Antonella De Angeli. 2004. My password is here! An investigation into visuo-spatial authentication mechanisms. *Interacting with Computers* 16, 6 (2004), 1017–1041.
[40] Karen Renaud and Melanie Volkamer. 2015. Exploring mental models underlying PIN management strategies. In *2015 World Congress on Internet Security (WorldCIS)*. 18–23. https://doi.org/10.1109/WorldCIS.2015.7359406
[41] Stuart Schechter and Joseph Bonneau. 2015. Learning assigned secrets for unlocking mobile devices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS)*.
[42] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.
[43] L'ubica Staneková and Martin Stanek. 2013. Analysis of dictionary methods for PIN selection. *Computers & Security* 39 (2013), 289–298.
[44] Elizabeth Stobert and Robert Biddle. 2014. The password life cycle: user behaviour in managing passwords. In *10th Symposium On Usable Privacy and Security (SOUPS)*.
[45] Emanuel Von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. Swipin: Fast and secure pin-entry on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*.
[46] Emanuel Von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2013. Survival of the shortest: A retrospective analysis of influencing factors on password composition. In *IFIP Conference on Human-Computer Interaction*. Springer.
[47] Ding Wang, Qianchen Gu, Xinyi Huang, and Ping Wang. 2017. Understanding human-chosen pins: characteristics, distribution and security. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. ACM.
[48] Zhi Xu, Kun Bai, and Sencun Zhu. 2012. Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors. In *Proceedings of the 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks*.

APPENDIX

A SURVEY MATERIAL

A.1 Closed Response Demographic Questions

(1) What is your age?
(a) 18-25; (b) 26-30; (c) 31-35; (d) 36-40; (e) 41-45; (f) 46-50; (g) 50+ yrs; (h) Prefer not to answer
(2) What is your identified gender?
(a) Male; (b) Female; (c) Non-binary; (d) Other; (e) Prefer not to answer
(3) What is your highest level of education?
(a) Some high school; (b) High school; (c) Some college/university; (d) Trade/technical/vocational training; (e) Associate's degree; (f) Bachelor's degree; (g) Master's degree; (h) Professional degree; (i) Doctorate; (j) Prefer not to say
(4) What is your annual household income?
(a) Under $15,000; (b) $15,000 – $29,000; (c) $30,000 – $49,999; (d) $50,000 – $74,999; (e) $75,000 – $99,999; (f) $100,000 – $150,000; (g) over $ 150,000; (h) prefer not to answer
(5) Which of the following best describes your educational background or job field?
(a) I have an education in, or work in, the field of computer science, computer engineering or IT;
(b) I do not have an education in, nor do I work in, the field of computer science, computer engineering or IT;
(c) prefer not to answer
(6) Which of the following best describes your level of proficiency with technology?
(a) Basic (I can perform basic tasks on a smartphone/laptop such as sending emails or browsing the internet;
(b) Intermediate (I can perform intermediate tasks on a smartphone/laptop such as changing the settings or installing new applications);
(c) Advanced (I have knowledge of and am capable of writing source code);
(d) Prefer not to answer
(7) Which of the following best describes your level of proficiency with security?
(a) Basic (I have a limited understanding of security i.e., does not know what antivirus is or does not know how to use it);
(b) Intermediate (I have some knowledge on aspects of security and different threats that exist and how to remediate some of them);
(c) Advanced (I have some formal training or actively researches security topics);
(d) Prefer not to answer
(8) Can you identify which of these relationships types apply to those you currently live with (choose all that apply)?
(a) Alone; (b) Spouse; (c) Own children; (d) Parents; (e) Siblings; (f) Friends; (g) Roommates; (h) Other (please describe the relationship type); (i) Prefer not to answer
(9) I live in an area that is: (*5-point Likert scale "Very safe"– "Very unsafe"*)
(10) I work or spend time in an area that is: (*5-point Likert scale "Very safe"– "Very unsafe"*)

A.2 Semi-structured Interview Questions

Asset Category Independent Questions: Part I.

(1) Can you please tell us how many unique PINs you currently use?
(2) Which resources do those PINs protect? For ATM cards, does the PIN protect one or multiple ATM cards?
[Participants were reminded of some assets that are commonly protected by a PIN. The list included ATM cards, smartphones, laptops, personal computers, online accounts, electronic home locks, home security systems, garage door openers, cars, bike/gym locks, voicemail, gaming consoles, apps, smartwatches, thermostats, and other home devices.]
(3) Did you miss any PINs previously? What resources do they protect?

Asset Category Dependent Questions. The following questions were repeated for each of the three PIN categories (digital, financial, and physical). Context-dependent questions were for the most frequently used PIN in each category, unless otherwise noted.

(1) Who else have you shared this PIN with? If friends or roommates, how many?
(2) How concerned would you be if your PIN was revealed to the following people: (*5-point Likert scale "Very concerned"– "Not concerned at all"*)
(a) Friends, (b) Roommates, (c) Parents, (d) Siblings, (e) Spouses, (f) Children
(3) How long have you been using this PIN?
(4) Have you ever changed a PIN in this category in the past? If so, what prompted it?
(5) **[IF CHANGED PIN]** What are your strategies for changing a PIN and picking a new PIN?
(6) Can you rank how important the security of this asset is you? (*5-point Likert scale "Very important"– "Not important at all"*)
(7) When picking the PIN, what was the order of importance for the following criteria: (a) memorability; (b) ease of usability; (c) security; (d) reuse of a previous PIN
(8) How often do you enter a PIN for this category?
(9) (For any asset in this category) Has there ever been a situation where someone learned your PIN? If so, who? How did they learn it? What device? What was your recourse? If the PIN was not updated, why?
(10) (For any asset in this category) Have you ever been in a situation where you were worried about someone observing your PIN? What was your recourse?
(11) (For any asset in this category) Have you ever been in a situation where you were worried about someone may try guessing your PIN? What was your recourse?
(12) (For any asset in this category) Have you ever shared a PIN with someone in the past that you are no longer in a relationship with? If so, who? [Examples include past spouses, friends, coworkers, and roommates]
(13) **[IF SHARED WITH PAST RELATIONSHIPS]** Did you take any steps to ensure that such people no longer have access to your PIN protected resources? What steps did you take, and why?

(14) Have you ever tried to learn or observe a PIN of someone? How? Was it successful? What resource were you trying to access? Was it someone you knew?
(15) If we ask you to guess the PIN of a person you know in five guesses, what strategies will you take?
(16) Would your strategies for the above question change if it was a stranger?
(17) (For any asset in this category) Do you store or write PINs anywhere, like a notepad or online password manager? If you write them on a notepad, where do you store it?

Asset Category Independent Questions: Part II.

(1) Have you ever used the same PIN for two or more devices? How about devices that are in different classes?
(2) Consider a digital device you use to login to your banking website/app or your digital wallets like Apple Pay or Google Pay. Is this device protected using a PIN (including PIN backup for fingerprint? If so, does access to your banking website or your digital wallets require another PIN or a password?
(3) How were the physical PINs to home or garage access were setup? [Did they set them up? Did they updated them when they moved to a new place? Did a technician set them up? Did the previous owner set them up or is it the default PIN? If the previous owner set up the garage door PIN, did they change key locks? If so, why not other PINs?]