# A Quest for Inspiration: How Users Create and Reuse PINs

Maria Casimiro, Joe Segel, Lewei Li, Yigeng Wang, Lorrie Faith Cranor
*{mdaloura, jsegel, leweil, yigengw}@ andrew.cmu.edu, lorrie@cmu.edu*
*School of Computer Science, Carnegie Mellon University*

## Abstract

Personal Identification Numbers (PINs), required to authenticate on a multitude of devices, are ubiquitous nowadays. To increase the security and safety of their assets, users are advised to create unique PINs for a lot of accounts they possess. Considering the multiple accounts users hold, remembering a myriad of PINs is often burdensome for users. As a consequence, we suspect users tend to trade-off security for memorability, due to the fear of forgetting their PINs, thus reusing them. To test this hypothesis we conducted a study on MTurk that asked participants about their PIN creation and reuse behaviors. Our results show that users draw inspiration from important dates to create their PINs and that PIN reuse is common practice, even between high and low valued accounts. Participants justify this behavior stating they reuse PINs for convenience and ease of remembrance.

## 1 Introduction

Personal Identification Numbers (PINs) are ubiquitous nowadays. Despite the fact that users are able to take advantage of more sophisticated authentication methods that use biometric data, they are still generally required to set up a backup/recovery PIN [9, 15]. Due to their omnipresence and to the fact that PINs are generally considered easier to enter than passwords [11], they are usually leveraged in situations where users are expected to be quick at performing a given operation, e.g., unlocking a mobile device. PINs have also become a standardized authentication method for banking purposes due to their ease of use on a number pad [5, 19], without requiring a full keyboard. As such, ensuring their safety and security is paramount. In contrast to passwords, PIN authentication is often used alongside heavy rate-limiting and strict lockout policies. However, despite these additional safeguards, Bonneau et al. [2] concluded that a guessing attack through the space of actually used PINs would be a practical approach for an adversary to gain access to victims' bank accounts. In fact, PINs are generally considered simple to guess by an adversary since users tend to pick easily memorable PINs, such as meaningful dates [2]. Figurska et al. [7] confirmed that people are not good random number generators. As such, PINs' "easy to remember" usability requirement is at odds with the "hard to guess" security requirement [12].

Previous studies have researched the capabilities of human memory with respect to memorizing PINs [1,3,6,8,10]. Given their purpose of making systems secure, they can only succeed if they comply with at least two criteria: being hard to guess and easy to remember. Although these works showcase the capabilities of the human mind, namely in terms of its ability to remember digits, they open new questions such as *"If humans are capable of remembering so many digits, why do they tend to reuse the same PINs?"* or *"Why do humans create PINs according to the same patterns?"* With respect to PIN security, past studies researched alternative ways of entering/using PINs, searching for more secure, easier to use options [4, 14, 20]. Yet, and unlike password reuse [16] which has been extensively researched, to the best of our knowledge the literature does not directly study how PIN reuse and the inspirations for the creation of PINs affect PIN security [15].

In this paper, we describe an MTurk survey that aims to provide a better understanding of *why* users reuse their PIN numbers, *where* they reuse their PIN numbers, and *which inspirations* they use to create their PINs. For this purpose, we define a set of usage scenarios, including credit/debit card, bike lock, cell phone, among others, and ask users to tell us for which scenarios they use PINs. Then, we ask them if they reuse their PINs and, in case they do, in which other scenarios they reuse them. One would expect that, for scenarios such as credit/debit cards and banking, users would have different


*Who Are You?! Adventures in Authentication (WAY)* 2020.
August 7, 2020, Virtual Conference.

PINs, exclusive for those scenarios. Our study shows that users in fact reuse these PINs in low-value accounts, thus compromising their most valuable assets. We further confirm that the most common inspirations employed by users are *birth dates* and *previously used PINs*. These findings are in accordance with previous password studies [18]. Nonetheless, the study of PINs as a separate topic is important due to the intrinsic differences between passwords and PINs such as the space of possible options (only numbers vs numbers, letters, symbols) and the size (4 digits for the most common PINs vs at least 8 characters for most passwords). Our results can be leveraged by the community to improve user awareness about the dangers of reusing PINs and of using known dates and other trivial inspirations to create PINs.

## 2 Methodology

In this section we start by describing our research questions. Then, we introduce our data collection and analysis methodology. For conducting our study, we recruited 150 individuals to take part in an online survey which asked users about their use of PINs in their daily lives. The survey asked participants about PIN use and reuse, and about their inspirations when creating new PINs, as well as demographic information. Over the course of this study, no personally identifiable information nor users' real PINs were collected.

### 2.1 Research Questions and Hypothesis

In this study we were interested in understanding users' behavior in terms of how they used their PINs, whether PIN reuse was frequent or not and what they were inspired by when creating their PINs. To understand whether users' behaviors pose security threats, we define the concept of *'value group'* as *'the set of scenarios users view as equally worthy of protection'*. We defined the following research questions:

**RQ1:** Do users reuse their PINs across value groups? How?

**RQ2:** What inspires users to create their PINs?

**RQ3:** How do people reuse their PINs' inspiration across value groups?

### 2.2 Recruitment

Participants were recruited through Amazon's Mechanical Turk crowd-sourcing service (MTurk) and were directed to the survey via a Qualtrics link. We posted an Amazon MTurk HIT (Human Intelligence Task) with payment of $1.25 upon completion of the survey and required each participant to be located in the US, have at least a 95% HIT approval rating, and be at least 18 years of age. Carnegie Mellon University's Institutional Review Board (IRB) approved our study. The median survey completion time was 5mins. and 13secs.

### 2.3 Survey

Our survey was hosted on Qualtrics. Our goal was to understand each individual's PIN use/reuse behavior, so we gave participants a list of scenarios for which they might use PINs and asked them to select the ones that applied to them. Tables 1 and 2 show all the scenarios participants could select. Prior to the start of the survey, we defined PIN as *a specific kind of password that is limited to numerical digits*. Then, for the remainder of the survey, we only asked questions about the scenarios that applied to each participant. Thus, the length of the survey varied for each participant. Participants that used PINs in more scenarios were asked more questions. Our survey was organized into five different sections.

**Current Use.** This section asked users to indicate all unique scenarios for which they currently use PINs, as well as the total number of PINs they regularly depend on. We decided not to group similar scenarios, such as cell phone and laptops, or credit/debit cards and banking, since participants could value them differently. By grouping them together, these nuances would be lost and there would not be the possibility of understanding reuse across value groups as profoundly. We further asked participants to report their total numbers of PINs (reuse) and unique PINs (no reuse).

**Risk.** This section had the purpose of defining the value groups, i.e., determining the scenarios users valued the most/least. We expected the most valued scenarios to correspond to those for which a user would feel at risk (financial, emotional, physical) should the PIN be discovered by an attacker. Thus, using a 5-point *Likert* scale, users were asked to state how they felt about the potential *physical*, *financial*, and *emotional* harm should an attacker discover their PINs.

**Reuse.** Next, we had users reflect about their PIN reuse behavior by asking if they reused PINs, and, for the scenarios for which they stated they did reuse PINs, what were the other scenarios that had the same PIN. We explicitly distinguished between *exact PIN reuse* and *partial PIN reuse*. The former corresponds to scenarios for which participants reused exactly the same PIN, i.e., no difference whatsoever between PINs. For the latter, we defined PIN variations by listing examples such as reordering numbers, changing only one digit, among others. These questions were open-ended.

**Inspiration.** This section asked users to select for each scenario what was the inspiration behind the creation of each PIN. The available inspiration options are listed in Table 3.

**Demographics.** The last section asked for demographic information (age, gender, education level, and profession).

### 2.4 Data Analysis

We checked the MTurk IDs and removed 2 of the 150 participants who appeared multiple times. Since our survey had both open-ended as well as multiple choice and *Likert* scale ques-

tions, we performed quantitative and qualitative data analysis. Next, we describe the methods employed to analyze the data.

**Quantitative Data.** We defined value groups to measure how important it is for the user that the PIN corresponding to each scenario is not discovered. We then assigned each scenario to either a *low value group* or a *high value group*.

**Qualitative Data.** To analyze the qualitative data corresponding to the open-ended questions, we used emergent coding. We created three codebooks, one for each open-ended question in the survey. Each codebook was developed iteratively by searching the answers for common themes. Two team members reviewed the responses individually and then resolved all conflicts. The average Cohen's kappa, a commonly-used statistic reflecting agreement among coders, was 0.76, suggesting a substantial level of agreement between coders [13].

## 2.5 Demographics

Out of the 148 valid responses, approximately 59.5% corresponded to male participants, 39.2% to female and 1.3% to non-binary. The average age was 38 years, the median was 35 and the mode was 28. In terms of education, most participants were college educated (74%). The last piece of demographics information collected was about the participant's profession. Less than 10% of the participants had IT jobs, and approximately 12% were in the Sciences, Technology, Engineering and Math sector.

# 3 Results

This section presents the results of our data analysis. We describe how value groups are formed and how these groups characterize users' behavior and attitudes towards PIN reuse.

## 3.1 Determining Value Groups

In order to determine the scenarios users valued the most, we asked participants to rate, using a 5-point *Likert* scale, how they valued each scenario for which they used a PIN along three different dimensions: physical, financial, and emotional. Then, by converting the *Likert* scale to scores (Completely Disagree - 1pt, Somewhat Disagree - 2pt, Neither Agree nor Disagree - 3pt, Somewhat Agree - 4pt, Completely Agree - 5pt), we calculated the average scores of each scenario for the three categories, which we show in Table 1. For each of the three dimensions, in order to determine whether a scenario was low or highly valued by participants we computed the median score of all scenarios. Based on this threshold, we then assigned scenarios with scores above the threshold to the *high value group* and scenarios with scores lower than or equal to the threshold to the *low value group*. The value groups are represented in Table 1 by the bold font, i.e., average scores shown in bold correspond to *high value groups* while scores shown in normal font correspond to *low value groups*. We

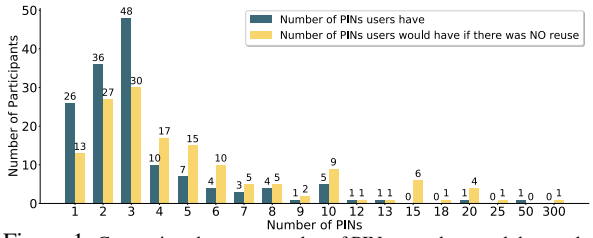


Figure 1: Comparison between number of PINs users have and the number of PINs users would have if there was no PIN reuse.

| **Scenario**<br>Value group threshold | **Physical**<br>2.64 | **Financial**<br>3.76 | **Emotional**<br>3.69 |
|---|---|---|---|
| Voicemail | 1.64 ± 1.08 | 1.87 ± 1.28 | 3.22 ± 1.50 |
| Gym locker | 2.17 ± 1.11 | 2.67 ± 1.44 | 2.92 ± 1.44 |
| Luggage | **2.69 ± 1.60** | 2.69 ± 1.49 | 3.62 ± 1.56 |
| Bike lock | **3.00 ± 1.52** | 3.14 ± 1.56 | 3.64 ± 1.39 |
| Cell phone | 2.51 ± 1.47 | 3.64 ± 1.26 | **3.99 ± 1.19** |
| Home entry | **4.48 ± 0.91** | 3.73 ± 1.13 | **3.94 ± 1.41** |
| Lock box | **3.22 ± 1.64** | **3.78 ± 1.48** | **3.89 ± 1.17** |
| Sim cards | **3.53 ± 1.06** | **3.87 ± 1.13** | 3.60 ± 0.83 |
| Laptop | **2.95 ± 1.62** | **3.90 ± 1.11** | **4.21 ± 1.04** |
| Safe | **3.36 ± 1.47** | **4.25 ± 0.93** | **4.14 ± 1.11** |
| Online account secure pin | 2.49 ± 1.64 | **4.30 ± 0.95** | **3.79 ± 1.38** |
| Banking (online/phone) | 2.59 ± 1.48 | **4.49 ± 0.92** | 3.54 ± 1.56 |
| Debit/credit cards | 2.55 ± 1.55 | **4.52 ± 0.92** | **3.74 ± 1.36** |

Table 1: Average value scores and standard deviation for each scenario. Average scores shown in bold correspond to *high value groups*.

see that the three scenarios participants appeared to value the most were *Laptop*, *Lock box*, and *Safe*, since all three dimensions were assigned to the *high value group*. A similar analysis shows the scenarios participants value the least are *Gym locker* and *Voicemail*, which were assigned to the *low value group* across all three dimensions. The remaining scenarios are highly valued only for some of the dimensions.

## 3.2 PIN Reuse Behavior

To get a preliminary idea of how frequent PIN reuse was, the first two survey questions asked participants for the number of PINs they currently used and the number of PINs they would use if there was no reuse. Figure 1 highlights that the majority of the surveyed participants has between 1-3 PINs. The pattern followed by both the blue and yellow bars suggests that participants reuse these PINs across scenarios, seeing as the yellow bars are shifted to the right. This shift means that users reported requiring more PINs when asked for the number of PINs they would have if they did not reuse them. To analyze users' reuse behaviors, we define two dimensions: PIN reuse across scenarios and types of PIN reuse.

**Reuse across scenarios (RQ1).** We were interested in understanding across which scenarios users reused their PINs. In particular, we wanted to get a sense of how common reuse between value groups, which poses a larger threat to high value accounts, was. Thus, we asked participants to report, for each scenario in which they used a PIN, if they reused that PIN in some other scenario. In case of an affirmative

| Scenario | Exact reuse | Partial reuse | % Participants |
|---|---|---|---|
| Home entry | 30% | 15% | 22% |
| Luggage | 46% | 46% | 9% |
| **Banking (online/phone)** | **48%** | **20%** | **57%** |
| **Debit/credit cards** | **52%** | **22%** | **89%** |
| Safe | 54% | 31% | 19% |
| **Laptop** | **55%** | **23%** | **55%** |
| Online account secure pin | 58% | 29% | 36% |
| **Cell phone** | **60%** | **26%** | **77%** |
| Gym locker | 67% | 42% | 8% |
| Voicemail | 67% | 15% | 37% |
| Sim cards | 73% | 47% | 10% |
| Lock box | 78% | 33% | 6% |
| Bike lock | 79% | 29% | 9% |

Table 2: Percentage of PIN reuse for each reuse type and of participants that reported having a PIN for each scenario. Scenarios in bold correspond to those for which the majority of participants reports having PINs.

answer, we asked a follow-up question to understand which was the scenario in which they reused their PINs. Since these questions were open-ended, each response was checked for basic understanding and placement into the correct group.

We found that participants tended to reuse PINs across scenarios which they valued equally for at least two of the value dimensions, usually physical and emotional. However, we also found reuse between high and low value groups. Voicemail was the scenario whose PIN was most reused on other scenarios, namely in high value scenarios such as laptop and safe, and in scenarios such as credit/debit card, banking, and online account secure PIN. An example of such a case is reuse between voicemail and credit/debit card. Although only 5% of participants fall under this category, it is still noteworthy, given the security threat of reusing the high value account PIN in a low value account, which typically has much weaker protections, in particular in terms of rate-limiting and lockout policies. Thus, this means that, for the case of our population, 5 out of 100 users might be vulnerable to having their credit/debit card PINs compromised by attackers first compromising the much easier-to-defeat voicemail account. We noticed similar percentages for reuse between online account secure PIN and voicemail, and also for laptop and voicemail. Additionally, of the 8 participants who stated they reused their exact gym locker PIN (low value group), 3 stated they reused this PIN either in their safe, credit/debit cards or for banking purposes. As such, the first take-away from our study is that ***Users reuse PINs regardless of their value groups.*** Seeing as the most reused PINs are the ones of the scenarios for which most participants reported having PINs (Table 2), this data seems to suggest that reuse is preponderant among the most frequently used scenarios, regardless of how users perceive the importance/dangers associated with those accounts.

**Types of PIN reuse.** We defined two types of reuse: reusing the exact PIN and reusing a slightly varied version of the PIN (e.g. reordering numbers, changing each number by the same amount, changing one digit). Table 2 shows the breakdown of PIN reuse into these categories, along with the percentage of users that reported having PINs for each scenario.

The analysis of the table allows us to draw three main conclusions: *(i)* when users reuse PINs, they tend to reuse the exact same PIN; *(ii)* for the majority of the scenarios (11 out of 13), at least half of the participants reuse the exact PIN for that scenario; *(iii)* the scenarios for which most users have PINs (shown in bold font in the table) coincide with some of the most valued scenarios (e.g.: laptops) and carry high percentages of exact reuse. These observations corroborate the previous example of how high valued accounts can be compromised through low value accounts, and highlight users' vulnerabilities due to unsafe behaviors.

## 3.3 Reasons for PIN Reuse

To understand what led users to reuse their PINs across scenarios, one open-ended question in the survey asked participants directly why they reused their PINs. We coded the participants' answers and found that the majority (55%) stated "easier to remember" as the reason for reuse. The second most common reason was "convenience", with 23% of participants reporting it. In fact, one of the participants whose answers we classified as belonging to the "easier to remember" category stated that "I reuse pins because its easier to remember and they have worked well for me." and two other stated that "I reuse those pins because they are easy to remember. I would rather memorize them instead of write them down." and that "Memorable and I haven't found a manager that works for me." These last quotes clearly highlight a trade-off between one insecure behavior for another and that current tools for storing sensitive information still do not match all of users' expectations and/or needs. This issue requires further research and is complementary to our study. As for the participants categorized under "convenience", we highlight the following statements: "What made me reuse the pin is that I was already adapted to it and its registered to my head already." and "Because I do not want to remember different PINs and/or passwords." These statements are in accordance with Renaud and Volkamer's results [17] who showed that users' PIN management strategies are not susceptible to change.

## 3.4 PIN Inspirations

To better understand what drives and inspires users when creating their PINs, we asked users to select from a set of predefined options what inspired them. Thus, for each scenario, we obtained the counts of each PIN inspiration, which we show in Table 3. Note that each participant was allowed to select multiple inspirations for the same scenario, thus the total count does not amount to the total number of participants.

**Most common inspirations (RQ2).** Table 3 shows that *important dates*, *reusing previous PINs* and *random numbers* were the most popular inspirations for creating PINs. These inspirations pose threats to users' accounts for several reasons: *(i)* people have been shown not to be good random number generators [7], thus, unless users leverage random number

| Inspirations \ Scenarios | Cell phone | Laptop | Debit/credit cards | Banking (online/phone) | Luggage | Sim cards | Home entry | Bike lock | Safe | Gym locker | Lock box | Voicemail | Online account secure PIN | Total count |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Random numbers** | 28 | **19** | **39** | **24** | 1 | **5** | **11** | 5 | **9** | 2 | **3** | **14** | 10 | 170 |
| **Important dates** | **29** | 18 | 25 | 16 | 2 | 0 | 7 | **6** | 4 | 1 | 0 | 12 | **12** | 132 |
| **Reusing previous PIN** | 18 | 15 | 22 | 10 | 2 | 2 | 2 | 1 | 4 | 0 | 2 | 8 | 10 | 96 |
| **Specific pattern on keypad** | 14 | 10 | 8 | 5 | **3** | 2 | 6 | 1 | 2 | 1 | 2 | 5 | 6 | 65 |
| **Phone numbers** | 5 | 11 | 10 | 6 | 0 | 2 | 3 | 1 | 2 | 1 | 2 | 3 | 3 | 49 |
| **Government issued numbers** | 8 | 2 | 7 | 8 | 1 | 1 | 4 | 0 | 3 | 1 | 1 | 4 | 8 | 48 |
| **House numbers** | 6 | 6 | 7 | 3 | 0 | 2 | 2 | 0 | 2 | 1 | 0 | 3 | 2 | 34 |
| **Zip codes** | 5 | 7 | 0 | 5 | **3** | 3 | 1 | 0 | 0 | 1 | 1 | 2 | 1 | 29 |
| **Addresses** | 5 | 1 | 6 | 4 | 0 | 0 | 2 | 0 | 0 | 0 | 1 | 1 | 2 | 22 |
| **Jersey numbers of athletes** | 3 | 2 | 4 | 5 | 1 | 0 | 1 | 0 | 1 | 0 | 2 | 0 | 0 | 19 |
| **Other** | 15 | 7 | 25 | 16 | 1 | 1 | 4 | 1 | 4 | **4** | 1 | 8 | 10 | 97 |

Table 3: Most common inspirations as a function of the scenarios. The bold font highlights the inspirations with highest count for each scenario.

generators, their random PINs are likely to be predictable; *(ii)* important dates are not only susceptible to targeted attacks, but also the space of PINs following date formats is relatively small; *(iii)* reusing previous PINs might lead users to assign compromised PINs to new accounts. This shows that, despite the known dangers of using, for instance, important dates for high value accounts, such as *Credit/debit cards* [2], participants do not heed the warnings of the security experts.

**PIN inspirations across value groups (RQ3).** Table 3 shows that, for the scenarios that are highly valued by participants, such as *Laptop*, *Debit/credit cards*, *Safe*, and *Online account secure PIN*, the most used inspiration tends to be random numbers. However, for most of these scenarios, important dates follows closely behind. Moreover, for the scenarios for which the majority of participants reported having PINs, like *Cell phone* and *Banking*, the number of participants that states using important dates and reusing previous PINs as inspirations is rather high. These data indicate that ***Users may reuse PIN inspirations across value groups***. Thus, further education of users and new PIN management strategies may be needed. Future work is required to statistically verify this hypothesis.

## 4 Discussion

This section discusses the limitations of our study, the results we obtained and interesting directions for future work.

**Limitations.** In this study we aimed at studying users' PIN reuse behaviors and inspirations. For this purpose, we conducted a survey on MTurk which explored different PIN use scenarios. Our results may have been affected by the fact that our participant pool was skewed towards young males, and college educated participants. Also, we highlight the possibility of users not being truthful when answering, due to fear of being judged for having unsafe behaviors when managing their PINs and which they know are unsafe. This is particularly relevant for the open-ended questions. Still, the data provide interesting insights into the mindset and behaviors of users. One other limitation of our study is the fact that users were only requested to answer questions regarding scenarios for which they had PINs, despite perhaps having opinions about other scenarios. This was a design choice whose purpose was to decrease the duration of the survey and prevent users from getting bored and start answering randomly. However, it also caused a lot of subgroups to appear, thus leading to some scenarios having substantially more answers than others (Table 2). These subgroups seem to skew PIN reuse towards more physical scenarios, such as *Gym locker* and *Bike lock*, which coincide with those for which only about 10% of participants reported having PINs. This limitation highlights the need for additional studies that address the problem of reuse patterns beyond these value groups. Finally, we believe demographics might affect PIN inspirations however, as our results do not allow us to draw conclusions regarding this hypothesis, we leave it for future work.

**Discussion.** One interesting aspect, and worthy of discussion, is related to the need for different PINs for each scenario. Undoubtedly, the most secure approach is to have different PINs for all scenarios. However, to accommodate users' memory capabilities, a viable approach to deal with the growing number of PINs is to allow PIN reuse for scenarios that are unlikely to be targeted by the same attacker. For instance, a person that is likely to rob your *Gym locker*, is unlikely to steal your *Luggage*. In this example, the danger of reuse does not seem to be as significant as when considering reuse across *Credit/debit cards* and *Voicemail*. This aspect should be further investigated, perhaps through the definition of specific guidelines of when PIN reuse is acceptable, along with a quantitative study of the likelihood of suffering successful PIN stealing attacks in each reuse case. Furthermore, one aspect which our study does not address is that of how cultural differences may affect PIN inspirations and creation strategies. This is a relevant aspect and past studies [21] have shown that different cultures have different strategies for PIN creation.

## 5 Conclusion

In this work we presented a study on users' PIN creation and reuse patterns. We defined PIN usage scenarios and introduced a metric called *value groups* to measure how important each scenario was for the users and to quantify the participants' will to protect the corresponding PIN. We expected that for scenarios users value the most along all dimensions (e.g. laptop and safe) the PINs for those scenarios would be unique. However, we found that participants in fact reuse those PINs, including across low value and high value scenarios.

With respect to users' inspirations, we expected important dates to be among the most common sources of inspiration and that users would leverage these to create PINs of scenarios belonging to the low value group, given the decreased security of PINs inspired by easily discoverable data. The data we collected allowed us to confirm that the most popular inspirations were in fact *important dates* and *reusing previous PINs*. Yet, it also showed that people reuse their PIN inspirations regardless of how they value each scenario.

**Acknowledgments.** Support for this research was provided by FCT (Portuguese Foundation for Science and Technology) through the CMU-Portugal Program.

## References

[1] Francis S Bellezza, Linda S Six, and Diana S Phillips. A mnemonic for remembering long strings of digits. *Bulletin of the Psychonomic Society*, 30(4):271–274, 1992.

[2] Joseph Bonneau, Sören Preibusch, and Ross Anderson. A birthday present every eleven wallets? the security of customer-chosen banking pins. In *Procs. of FC*, pages 25–40, 2012.

[3] Nelson Cowan. The magical number 4 in short-term memory: A reconsideration of mental storage capacity. *Behavioral and brain sciences*, 24(1):87–114, 2001.

[4] Antonella De Angeli, Lynne Coventry, Graham Johnson, and M. Coutts. Usability and user authentication: Pictorial passwords vs. pin. *Discovery*, 01 2003.

[5] Alexander De Luca, Marc Langheinrich, and Heinrich Hussmann. Towards understanding atm security: a field study of real world atm use. In *Procs. of SOUPS*, 2010.

[6] Tam Joo Ee, Chua Yan Piaw, and Loo Fung Ying. The effect of rhythmic pattern in recalling 10 digit numbers. *Procedia-Social and Behavioral Sciences*, 185:400–404, 2015.

[7] Małgorzata Figurska, Maciej Stańczyk, and Kamil Kulesza. Humans cannot consciously generate random numbers sequences: Polemic study. *Medical hypotheses*, 70(1):182–185, 2008.

[8] Andreas Gutmann, Karen Renaud, and Melanie Volkamer. Nudging bank account holders towards more secure pin management. *Journal of Internet Technology and Secured Transaction*, 4:380–386, 06 2015.

[9] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception. In *Procs. of SOUPS*, 2014.

[10] Jun Ho Huh, Hyoungshick Kim, Rakesh B Bobba, Masooda N Bashir, and Konstantin Beznosov. On the memorability of system-generated pins: Can chunking help? In *Procs. of SOUPS*, pages 197–209, 2015.

[11] Markus Jakobsson, Elaine Shi, Philippe Golle, and Richard Chow. Implicit authentication for mobile devices. In *Procs. of USENIX Hot topics in security*, volume 1, 2009.

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

[13] J Richard Landis and Gary G Koch. The measurement of observer agreement for categorical data. *Biometrics*, pages 159–174, 1977.

[14] Mun-Kyu Lee, Jin Bok Kim, and Matthew K Franklin. Enhancing the security of personal identification numbers with three-dimensional displays. *Mobile Information Systems*, 2016.

[15] Philipp Markert, Daniel V Bailey, Maximilian Golla, Markus Dürmuth, and Adam J Aviv. This pin can be easily guessed. *arXiv preprint arXiv:2003.04868*, 2020.

[16] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. Let's go in for a closer look: Observing passwords in their natural habitat. In *Procs. of CCS*, pages 295–310, 2017.

[17] Karen Renaud and Melanie Volkamer. Exploring mental models underlying pin management strategies. In *Procs. of WorldCIS*, pages 18–23. IEEE, 2015.

[18] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. "i added '!' at the end to make it secure": Observing password creation in the lab. In *Procs. of SOUPS*, 2015.

[19] Melanie Volkamer, Andreas Gutmann, Karen Renaud, Paul Gerber, and Peter Mayer. Replication study: A cross-country field observation study of real world {PIN} usage at atms and in various electronic payment scenarios. In *Procs. of SOUPS*, 2018.

[20] Emanuel Von Zezschwitz, Paul Dunphy, and Alexander De Luca. Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. In *Procs. of MobileHCI*, pages 261–270, 2013.

[21] Ding Wang, Qianchen Gu, Xinyi Huang, and Ping Wang. Understanding human-chosen pins: Characteristics, distribution and security. In *Procs. of Asia CCS*, 2017.

# APPENDIX

## A Survey Questions

***Description.*** The purpose of this survey is to understand the patterns used by people to create PINs and how people reuse their PINs across different scenarios. In this survey, we define PINs as a specific kind of password that is limited to numerical digits. In this survey, we are only asking questions related to your PINs.

1. For each of the following, please select the scenarios in which you use PINs. (Select all that apply)

   ☐ Cell phone ☐ Safe ☐ Gym locker
   ☐ Voicemail ☐ Laptop ☐ Debit/credit card
   ☐ Sim cards ☐ Lockbox ☐ Banking (online/phone)
   ☐ Bike lock ☐ Luggage
   ☐ Home entry (garage door, smart lock)
   ☐ Online account secure PIN
   ☐ Other (enter at most 1 scenario)

***PIN Reuse.***

2. How many PINs do you currently use? (If you use the same PIN in multiple places, only count it once)

3. Imagine you had different PINs for all the scenarios for which you need PINs. How many different PINs would you have?

***Value Groups.*** Participants were shown the following Likert-style options for the set of statements below:

| *Completely Disagree* | *Somewhat Disagree* | *Neither Agree nor Disagree* | *Somewhat Agree* | *Completely Agree* |
|---|---|---|---|---|

4. For each scenario, if my PIN was discovered by an attacker, I am at serious risk of **physical** harm.

5. For each scenario, if my PIN was discovered by an attacker, I am at serious risk of **financial** harm.

6. For each scenario, if my PIN was discovered by an attacker, I am at serious risk of **emotional** harm.

***PIN Reuse Across Scenarios.***

7. For each scenario, do you reuse the exact same PIN for one or more other scenarios? If 'Yes', where do you reuse your PIN?

   By "reuse", we mean reusing the exact same PIN with no changes.

   ☐ Yes _____ ☐ No

8. For each scenario listed below, do you use variations of the same PIN for one or more other scenarios?

   By 'variations,' we mean reordering numbers, changing each number by the same amount, only changing one digit, etc.

   ☐ Yes ☐ No

9. Consider the scenarios for which you reused PINs. What made you reuse that/those PIN(s)?

***PIN Inspirations.***

10. For each scenario, what inspired you to choose your PIN? (Select all that apply)

    ☐ Addresses ☐ Important dates
    ☐ House numbers ☐ Reusing previous PIN
    ☐ Phone numbers ☐ Jersey numbers of athletes
    ☐ Random numbers ☐ Specific pattern on keypad
    ☐ Zip codes ☐ Government issued numbers
    ☐ Other

***Demographics.***

11. Please enter your age.

12. Please select your gender.

    ☐ Male ☐ Female
    ☐ Non-Binary ☐ Not specified

13. What is your current profession?

14. Please select your Highest Degree of Education

    ☐ Some high school ☐ High School Diploma / GED
    ☐ Associate's Degree ☐ Some College (incomplete)
    ☐ Bachelor's Degree ☐ Currently attending college
    ☐ Master's Degree ☐ Doctoral or Professional degree