"Someone Definitely Used 0000": Strategies, Performance, and User Perception of Novice Smartphone-Unlock PIN-Guessers

Daniel V. Bailey
Ruhr University Bochum
Germany

Collins W. Munyendo
The George Washington University
USA

Hunter A. Dyer
The George Washington University
USA

Miles Grant
The George Washington University
USA

Philipp Markert
Ruhr University Bochum
Germany

Adam J. Aviv
The George Washington University
USA

ABSTRACT

We examine the risk to lost, stolen, or unattended smartphones due to attempts to guess the device's unlock PIN, the most widespread authentication scheme for smartphones. We find *novice* attacks by those lacking forensic tools or training to be common, with over one-third of survey participants (n = 210) admitting trying to unlock someone's smartphone without their knowledge in the past year. We further find these novice attacks to be surprisingly effective against PINs, with participants guessing roughly the PIN of 1 in 8 strangers. Our study also produces the first *attacking* PIN dataset, to our knowledge, obtained from participants guessing PINs of other participants. We additionally investigate participants' mental models for *how* and *when* PIN-guessing may be attempted, finding that most participants expect insiders (friends, family, partners) to be those most likely to attempt to access their smartphone, underestimating risks from strangers due to loss, theft or recycling of their devices.

ACM Reference Format:
Daniel V. Bailey, Collins W. Munyendo, Hunter A. Dyer, Miles Grant, Philipp Markert, and Adam J. Aviv. 2023. "Someone Definitely Used 0000": Strategies, Performance, and User Perception of Novice Smartphone-Unlock PIN-Guessers . In *The 2023 European Symposium on Usable Security (EuroUSEC 2023), October 16–17, 2023, Copenhagen, Denmark.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3617072.3617113

1 INTRODUCTION

Smartphones are extremely pervasive and store a great deal of sensitive and personal information [22] that must be protected. Unfortunately, their ubiquity means that these devices might be misplaced, left unattended or stolen, potentially falling into the hands of a stranger who might have the opportunity to guess the device's unlock PIN, password, or pattern. Even without the benefit of sophisticated forensic tools and training, how successful might these *novice* guessing attackers be? Even though these situations are commonplace, to our knowledge, no study has specifically investigated how effective novice attackers are in practice.

EuroUSEC 2023, October 16–17, 2023, Copenhagen, Denmark

ACM ISBN 979-8-4007-0814-5/23/10.
https://doi.org/10.1145/3617072.3617113

Prior work notes that PINs are the most widely used mechanism to secure access to smartphones, with about 60% of participants using PINs [30] to unlock their devices. Previous studies [30] have also shown that many human-chosen 4-digit PINs can easily be guessed by adversaries in just a few attempts, and that upgrades to 6-digit PINs, unfortunately, do not meaningfully improve security [30, 36]. At the same time, previous studies [14, 30, 36, 53] assume well-trained attackers with sophisticated tools, who represent only a small fraction of the population and might not model the capabilities of most people who encounter the locked smartphone of another on any given day. Additionally, millions of smartphones are lost or stolen each year in the U.S. [21] alone. By purchasing 228 second-hand phones from police auctions in the US, Roberts et al. [43] found that 21.5% of the phones were not locked at all with a PIN or pattern, while another 4.8% used top-40 most common PINs and patterns which the authors were able to easily guess and gain access to a lot of sensitive and personal information on the devices without using any forensics. This makes it important to explore how low-resourced attackers without any forensic expertise might perform when guessing unlock PINs.

Motivated by this under-explored threat model, we seek to address the following three research questions:

(1) How do participants select PINs when primed to guess the PINs of other participants?
(2) How well do novice attackers perform compared to the data-driven guessers used previously?
(3) What PIN-based smartphone-unlock scenarios are participants most concerned about?

To answer these research questions, we developed a simulated-attack methodology inspired by Uellenbeck et al. [50] who incentivized participants to guess Android unlock patterns chosen by others. We study PINs using an online survey: participants (n = 210) first select a "secret" PIN they would use to protect their smartphone. Thereafter, participants entered five guesses for PINs selected by others in the study, receiving a bonus payment if they succeeded in guessing any other participant's PIN. Each participant was assigned to one of two treatments, corresponding to 4- or 6-digit PIN selection and guessing. Each treatment had a total of 105 participants.

Even without hints or forensic tools, our novice attackers show remarkable success. For example, a novice attacker willing to enter the same five 4-digit guesses on 8 phones would expect to unlock at least one of them; a total of fourteen 4-digit PINs and seven 6-digit PINs were guessed. While prior work analyzing informed, data-driven attackers [30, 36, 55], found little to no benefit for 6-digit

over 4-digit PINs, our novices guessed fewer of 6-digit compared to 4-digit PINs. Note, we refer to attackers previously used by researchers [30, 36, 55] as data-driven as these approaches leverage large and well-optimized PIN datasets previously collected when guessing PINs.

We further compared our new *offensive* PIN dataset collected from novices to PINs collected by Markert et al [30] in previous work. In the aggregate, novices' PIN guessing performance is similar to the data-driven approaches used previously by researchers. Our work therefore provides experimental evidence supporting the guessing models in the literature. Specifically, when making up to 30 guesses, a novice attacker performs slightly better than data-driven attackers, guessing 8.1% of the 4-digit PINs collected by Markert et al., comparable to the 7.6% guessed by a data-driven attacker. Similarly, a novice guesser succeeds at guessing 9.6% of 6-digit PINs collected by Markert et al. after 30 guesses, again slightly more than 8.7% guessed by a data-driven attacker. Our results show that data-driven attackers indeed model real-world threats, and support the guessing approaches leveraged in previous studies [30, 36, 53].

Participants additionally explained their expectations around PIN security and guessing, and 45% of participants changed their smartphone PIN to *keep someone out*. Very few (7%) of our participants mentioned concerns about strangers or thieves, focusing instead on close social relations and perhaps underestimating the threat of the lost/stolen device scenario. About one-third (34%) of participants overall thought their PIN would be guessed in the study. For those whose PIN was guessed, once again one-third (33%) thought it would be, suggesting participants' perception of the risk of PIN guessing is not related to their PIN choice.

In summary, a lost, stolen, or unattended smartphone represents a target of opportunity. In this paper, we ask "how effective is a PIN in protecting a lost, stolen, or unattended smartphone?" This real-world scenario represents an opportunity for potential attacks by the general public who lack any specialized forensic training or tools, but still can try a few guesses. We conducted a user study exploring how novices guess PINs, yielding a unique new dataset of their guesses. We find that even novice attackers without any knowledge about the victim have surprising capacity to guess PINs. We additionally find that a third of participants had recently tried to gain unauthorized access and that even more had changed their PIN to keep people out. We offer recommendations for design interventions as well as user education to nudge users towards more secure PIN choices.

2 RELATED WORK

Security of Mobile Authentication. Prior work has analyzed the security of numerous knowledge-based authentication schemes used on mobile devices, for example, alpha-numeric passwords [34, 46], LG Knock Codes [45], and Android unlock patterns [5, 6, 9, 28, 35, 50]. While these studies [14, 30, 36, 53] consider optimized, data-driven attackers in the form of perfect knowledge and simulated attackers, our work focuses on the more commonplace PIN-guessing attacks by novices such as friends as these attackers have the most opportunities to access locked devices.

In their study of PINs, Bonneau et al. [14] focused their analysis on human-chosen 4-digit PINs which are predominant for mobile devices but are also used in the banking sector for payment cards. Wang et al. [53], Markert et al. [30], and Munyendo et al. [36] on the other hand, also included 6-digit PINs which are predominant in Asia and the default on Apple devices since the roll out of iOS 9 in 2015 [8, 20]. Their analyses show that the security of 4- and 6-digit PINs is comparable and in certain cases, 4-digit PINs are more secure. This is particularly the case for an online attacker limited in the number of guesses they can make, with general knowledge of the distribution of PINs, but no targeted knowledge about the victim. Munyendo et al. particularly highlight the limited security benefits of upgrading from 4- to 6-digit PINs. The study also notes that security-oriented messaging can lead to more secure PIN choices.

In addition to these untargeted attacks, there are also scenarios where the attacker has information about the victim, for example if their birthday is known [14, 55]. In other cases, the attacker obtains information through shoulder surfing [10, 12, 18, 19, 52, 56], smudges on the screen [11, 16], or thermal sensors [1]. For instance, Zarandy et al. [57] showed that voice assistants can be used to extract the PIN by collecting acoustic signals of the user typing.

The study with methodology most closely related to our work is the one by Uellenbeck et al. [50] that studied Android unlock patterns. In their in-person lab experiment, Uellenbeck et al. had participants create a "defensive" Android unlock pattern and then provided them with five attempts, or "offensive" patterns, to guess the defensive choices of other participants. Participants who either guessed a defensive pattern or selected a pattern that was not guessed within 20 minutes were rewarded with candy. Our method of PIN selection and guessing bears some similarities. In our case, we focus on PINs, and similarly offer an incentive (cash bonus) for those who successfully guess the "secret" PIN of any other participant. While the results and analyses of Uellenbeck et al. focus on Android patterns and propose interventions for better pattern selection, our analysis focuses on how participants choose, guess, and expect others to guess their unlock PINs, both 4- and 6-digit. We additionally highlight the threat models that participants are most worried about when it comes to access to their devices, notably friends and family, as opposed to thieves or strangers.

Smartphone Threat Models. While analyzing the distribution of PINs shows to what degree a PIN is guessable, it does not explain why users choose PINs this way. The fact that users are aware of their insecure behavior when asked about it was shown in a study by Harbach et al. [24] where most participants reported that unwanted access to their smartphone would have been possible. Similarly, Mahfouz et al. [29] observed an average auto-lock timeout of 65 s in their study, enabling an attacker to access a smartphone if the owner leaves it unattended and does not lock it manually. To mitigate such risks, Kraus et al. [27] recommended offering simple mechanisms which are secure by default. This could also prevent potential social pressure. Matthews et al. [33] presented a taxonomy of device-sharing scenarios while Alabayram et al. [3] highlighted risk awareness as a driving aspect for insecure behavior rather than inconvenience, suggesting the need to effectively communicate risks. A follow-up study with users in Saudi Arabia by Al Qahtani et al. [2] confirmed these results. Another study by Bailey et al. [13] showed that users of Signal with increased comprehension of the PINs' purpose selected more diverse PINs.

While in the present work we focus on the risk of successful guessing and users' mental models of the threats, Roberts et al. [43] showed the sheer amount of sensitive data that can be found on lost, stolen, or seized phones that are auctioned off to the public by police in the United States. Similar to our threat model, Roberts et al. conducted a guessing attack, successfully unlocking 4.8% of the devices they purchased from the auctions due to usage of common PINs and patterns on these devices. The distribution of lock schemes including type (PIN, password, something else) and PIN length are not reported and the origin of their list of PIN guesses is unclear, making exact comparisons difficult. Nevertheless, this work shows that this is an important threat model that warrants exploration.

Shi et al. [47] presented a two-fold threat model for mobile authentication based on an informed and uninformed stranger. Muslukhov et al. [37] extended Shi et al.'s model with capabilities such as physical access and shoulder surfing. They conducted a survey of threats perceived by smartphone users and find that participants were equally concerned about strangers and "insider" threat actors such as friends. Moreover, 12 % of the participants in their study had experienced someone accessing sensitive data without their permission; 9 % admitted doing so themselves.

Marques et al. [32] quantified the prevalence of snooping in a survey designed to minimize social-desirability bias. The survey defined snooping as "looking through someone's phone without their permission," finding 31% of participants had done so in the previous year. We adopt this mild phrasing in our survey instrument to characterize what may be seen as anti-social behavior, finding that 37% of participants had tried to access someone's device in the previous year. In subsequent work, Marques et al. [31] explicitly recruited participants who have past experience with unauthorized access. They found that distilling stories of unauthorized access into identifying the familiar who, what, and why categories led to interesting insights. Participants felt that making themselves vulnerable to unauthorized access was necessary to sustain relationships with friends, partners, co-workers, and others.

3 METHOD

3.1 Attacker Model

This work focuses on a novice throttled attacker relevant to Google's Android and Apple's iOS, where rate-limiting mechanisms are in place to slow or stop an attacker from trying every possible PIN. We refer to "secret" PINs chosen by device owners to defend against attacks and "guesses" or "guessing PINs" chosen by an attacker on offense. Our simulation considers the attacker successful if any of their five guesses matches the secret PIN of any other participant. We consider the results of each guesser entering the same guesses on 104 different devices. Given the lifetime of unlock PINs, we assume each PIN will face many instances of unattended attack opportunities. We make the following assumptions:

(1) The attacker is performing an *online* or *UI-bound* attack, limited in the number of guesses. Based on the throttling implemented on iOS 15, the phone locks after six incorrect guesses, so an attacker can make five guesses without locking the phone. Similarly on Android, after five guesses, the phone locks for 30 seconds [7].
(2) The attacker knows the secret PIN length, i.e., whether to guess a 4- or 6-digit PIN. This is the case for Apple devices where the GUI of the lock screen indicates the PIN length.
(3) The attacker is *untargeted* and *novice*, i.e., has no personal information about the victim whatsoever and uses their intuition to guess PINs others may have chosen. As described in Section 2, it has been shown that an attacker who has knowledge about the victim, by knowing their birthday for example, can use this knowledge to increase their success rate. Our guessability results, therefore, provide a lower bound on an attacker's capability.

3.2 Survey Structure

Here, we outline the survey structure. Please refer to Appendix A for a detailed description of the survey instrument including the full wording of all questions.

To allow comparison with previous work, we use the same language and similar ordering of prompts and tasks, the same general appearance and functionality of the PIN pad, and survey questions from previous studies. For example, the practice, task description, and creation prompts match those from Markert et al. [30] for the selection of secret PINs. The overall aim of this approach is to minimize additional bias that might be introduced due to question presentation, phrasing, or a different PIN pad. All participants were required to complete the study using a smartphone: their user-agent string was recorded to ensure a smartphone was used.

Further, we assigned participants to one of two PIN treatments (4-digits or 6-digits). The study itself was identical for both groups, differing only when creating, recalling, or guessing a PIN, with the PIN-pad layout requesting a 4- or 6-digit PIN. After assignment to their treatment, each participant completed the following:

(1) *Informed Consent*: On the landing page, participants were shown the consent form where we described the purpose and duration of the study as well as any anticipated risks. We also informed participants that they can withdraw from the study at any time without penalty.
(2) *Agenda*: This page described the overall layout of the study including the three main tasks of the study: (1) creating a PIN, (2) making five attempts to guess the PIN of other participants, and (3) completing a short survey.
(3) *Practice*: To ensure all participants were familiar with the PIN interface, we asked them to practice entering a PIN. The PIN length was set to 4- or 6-digit, depending on the treatment.
(4) *Task Description*: Participants were told the context for PIN creation, namely, to unlock their smartphone; and that the PIN should be remembered for the duration of the study without writing it down.
(5) *Creation*: On the page shown in Figure 5, participants created their secret PIN, and confirmed it to ensure against accidental mistyping. The layout of this page changed according to the assigned PIN length.
(6) *Creation Strategy & Perception*: Afterward, we asked participants about their creation strategy (Q1) and how they perceived it in terms of security, ease of entry, and memorability (Q2–Q4), following Markert et al [30]. Moreover, we asked participants if they reused one of their own PINs (Q6)

and if so, the context for this (Q7), following Khan et al. and Casimiro et al [15, 26]. In between these questions, we included an attention check (Q5).

(7) *Task Description*: Followed by the questions about their own secret PIN, we framed the guessing task as shown in Figure 6. We highlighted that the five guesses must be unique, that more than 100 participants would take the study, and any number of correct guesses would earn the bonus payment of $0.50.
(8) *Guessing*: As participants were now informed about the guessing task, they made their five guesses on the page shown in Figure 7. If participants provided the same PIN twice, we notified them that the guesses must be unique. Note, participants only guessed PINs of their assigned PIN length.
(9) *Guessing Strategy and Threat Model*: After the guessing procedure, we showed the participants their 5 guesses and asked them about their overall strategy when making these guesses (Q8). Afterward, we asked participants about a scenario in which others may try to access their smartphone, including their reasons, and the strategies employed (Q9). We also asked participants if they considered this scenario when creating their secret PIN or making their guesses (Q12 and Q13). With the next five questions (Q14 – Q18), we intended to learn about participants' perception and experience of someone accessing their smartphone.
(10) *Recall*: We now asked participants to recall their secret PIN. If they could not recall their PIN within three attempts, they advanced to the next step and were compensated normally and their data included in the evaluation.
(11) *Guessing Success*: We asked participants if and why they thought their secret PIN would be guessed as well as if and why they thought they guessed someone's PIN.
(12) *Demographics*: Questions D1 to D8 asked the age, gender, education and IT background of participants as well as their smartphone usage. To prevent interference of the participants' demographic background with the results, we asked these questions at the end, following survey best practices recommended by Redmiles et al [41].
(13) *Honesty*: We concluded the study by asking participants if they participated honestly. We highlighted that they would not be penalized in any sense if they indicated dishonesty. This approach has been taken with the prior work in this area in order to increase the quality of the data collected [13, 30, 36].

3.3 Recruitment and Demographics

We ran pilots in our labs to ensure the clarity of the questions and correctness of the data collection process. As a result, we made slight edits to the wording of some questions, leaving intact the "look and feel" of the PIN pads used in prior work. No data from the pilot studies was incorporated into the final results. For the main study, we recruited 226 participants through Prolific, restricting participation to those residing in the U.S. After excluding 16 participants who indicated dishonesty, we ended up with $n = 210$ participants, 105 for each PIN length. Participants were compensated $3.50 for completing the study, taking on average 13 minutes. In total, 179 participants correctly guessed at least one PIN and were compensated a $0.50 bonus payment for a total compensation of $4.00.

Table 2 depicts the demographics of our participants. The majority of participants were women (112; 53%) compared to men (90; 43%) or non-binary (8; 4%). As expected when using a crowdsourcing platform [39], participants tended to be younger, 73% below the age of 35, and more educated (59% had a Bachelor's degree or higher). The majority (143; 68%) reported that they did not have a technical background.

3.4 Ethical Considerations

To limit any negative implications resulting from our study and the data we collect through it, we took several steps. Foremost, our study and its design were approved by our Institutional Review Board (IRB). Further, we informed participants about the purpose of our study and required their consent to proceed. During the study, participants could opt out at any time without any consequences.

Regarding the data, it may have happened that participants selected their actual PIN during the study. We also asked participants in Q6 whether the secret PIN they selected is a PIN they actually use and a total of 58 participants (27%) affirmed. Although this supports the ecological validity of our data, it imposes the risk of harming the user. To mitigate this risk, we used the Prolific ID as the only identifier in our study and analyzed the PIN data separately from it. For Q9, we asked participants to describe a situation where someone might access their phone and if relevant include information about their relationship to this person. As this might pose a risk of participants including Personally Identifiable Information (PII), we explicitly told them not to include PII.

3.5 Qualitative Analysis

Each of our study questions that involved open-ended answers was reviewed by two independent coders in the following manner: A primary coder created a codebook and coded all responses. A secondary coder then used the codebook to code all responses. Cohen's κ was calculated for all questions, ranging from 0.825 to 0.926, indicating that coding was reliable. To reach consensus, we observed that some disagreements were lapses in code assignment by researchers; others were resolved by disambiguating and combining some code descriptions.

3.6 Limitations

Our study has several limitations. Foremost, as this was an online study, we could not fully ensure that participants followed our instructions completely. To mitigate this, we included open-ended text based responses as well as an attention-check questions. Additionally, participants could indicate if they did not participate honestly at the end of the study, without fearing any negative consequences. Through these questions, we identified 16 participants whose answers were excluded from the final analysis. As is typical for studies using Prolific or other crowdsourcing platforms, participants were younger and more educated. While the survey is not U.S. census-representative, Redmiles et al. [42] showed that

crowdsourced samples used by researchers are generally an effective proxy for conditions in the real world, especially for U.S. participants aged 18-49 with at least some college education. While we believe that our results reflect common user attitudes, additional work is required to determine how well these results generalize, especially for more-diverse user populations. For example, it has been shown that populations from other locales such as China select PINs with different distributions [53]. Our study focused on participants from the U.S. only, and additional work is required to study PIN guessing in other countries and cultures.

Similar to Uellenbeck et al.'s [50] study design, participants in our study knew from the agenda text seen in Appendix A that other users would attempt to guess their PIN—possibly yielding more secure choices. Participants also knew they would have to use and remember the PIN only for the short duration of the study, which may also have encouraged the use of more secure PINs. On the other hand, previous studies that have used a similar method collected generalizable authentication data [30, 51]. Moreover, unlike in Uellenbeck et al.'s study, we highlighted the bonus payment for correctly guessing other participants' PINs for the first time after participants had already created their secret PIN.

Some of our survey questions asked about behaviors that may not be seen as socially desirable. For example, participants were asked if they had ever tried to access someone else's smartphone without their knowledge and if they had ever changed their PIN to prevent someone from accessing their smartphone. In both situations, a participant could be seen as admitting undesirable behavior: in the first case by exceeding granted permissions, or in the second case by the need to perhaps conceal something. Our study cannot determine if participants were untruthful, except to note that responses to both these questions were roughly the same, and were somewhat consistent with previous studies.

4 RESULTS

4.1 RQ1: PIN Characteristics

PIN Features. The features of secret and guessing PINs can be categorized into four groups: *date*, *repeat*, *sequential*, and *pattern*. Table 3 in Appendix C provides a detailed breakdown for each category. Note, some PINs such as `0101` can match multiple patterns, including *date* and *repeat*. Overall, *date* is the most popular pattern for secret and guessing PINs for both 4- and 6-digit PINs, as seen also in prior work [14, 30, 36]. Dates throughout this section correspond to four different types of sequences, including `yyyy` for "recent year," defined as sequences 1940–2028, similar to the definition used by Wang et al [53]. Examining the 4-digit PINs shows that 11% of the secret PINs and 5% of the 4-digit guesses represent a recent year. Four-digit PINs of the format `mmyy` (beginning with digits 01-12) account for 26% of the secret PINs compared to 33% of the guesses. The format `mmdd`, which is particularly popular among the survey US population (cf. Section 3.3), accounts for 20% and 12% of secret and guessing PINs respectively for 4-digit PINs. Notably less PINs follow the format `ddmm`, 9% and 10%, respectively. For the 6-digit PINs, we similarly observe that the secret PINs and guesses follow the same patterns, with 37% of both secret and guessing PINs following the format `mmyyyy`. PINs in the format `mmddyy` account for 30% of secret PINs, but only for 16% of guessing PINs. Third, `yymmdd` accounts for 16% and 11% of secret and guessing PINs respectively. These results align with prior work [14, 30, 36] which found that dates represent a sizable portion of 4- and 6-digit PINs.

Table 1: Responses to Q6: Was the secret PIN that you entered a PIN that you use on your smartphone or other personal devices?

	4-digit		6-digit		Total	
	No.	%	No.	%	No.	%
Yes	34	32	24	23	58	28
No	68	65	73	70	141	67
Do not use PIN	3	3	6	6	9	4
Unsure	0	0	2	2	2	1

The most popular sequential feature across secret PINs is an ascending order, e.g., `1234` for the case of 4-digit PINs. However, it only accounts for 2% of the total 4-digit secret PINs. For both PIN lengths, only about 5% of all secret PINs follow this pattern, despite its popularity among the guesses. Our results further reveal that one in three 6-digit guesses depicts a rectangular walk on the PIN pad, e.g., `139713`, despite only 5% of the secret 6-digit PINs following this pattern. Guesses reflect the features imagined to be popular, which diverge from the actual secret PINs the participants selected.

Selection Strategies. When asked about the strategies used to create their secret 4- or 6-digit PINs, participants in both treatments often mentioned a *date* ($n = 33$; 31% for 4-digit and $n = 29$; 28% for 6-digit). This finding is in line with results from our PIN analysis as well as prior work [14, 30, 36]. However, the incidence of date-related responses was somewhat higher in the 4-digit PIN treatment compared to the 6-digit PIN treatment.

The second most frequent strategy in both treatments was *memorable*, i.e. choosing a PIN that is easy to remember ($n = 14$; 13% for 4-digit and $n = 19$; 18% for 6-digit), also in line with prior work [30, 36]. For instance, P3 mentioned that "it was just three 2 digit numbers i [*sic*] knew I'd remember."

Selecting a PIN based on something that had a *meaning* to participants was the next most common strategy. This was more prevalent for 6-digit PIN participants compared to 4-digit PIN participants ($n = 8$; 8% for 4-digit and $n = 14$; 13% for 6-digit). For example, P40 mentioned "using numbers that hold personal meaning to me but don't have to do with birthdays or anniversaries."

Participants in both treatments also indicated using a *pattern* for various reasons, including convenience. As an example of a pattern, P104 stated: "The shape or movement of my thumbnail, I drew a rocket ship with the numbers so I could use muscle memory to sign in and not worry as much about the numbers."

The use of *random* numbers and *reuse* of PINs were also frequently mentioned by participants, as well as creating a PIN that is *simple*. Other less frequently cited strategies included using *subsets* of phone numbers, *ZIP codes* and *words*.

PIN Reuse. Reusing credentials remains a challenge in online safety; therefore, we asked participants if they reuse their 4- or 6-digit PIN on any other accounts. Across both treatments, more

than half indicated they do not reuse their PINs. However, *reuse* was more prevalent for 4-digit PINs at 32% compared to only 23% of 6-digit PINs, as shown in Table 1. While this may suggest a possible benefit of 6-digit PINs, 4-digit PINs are more commonly used and are thus more likely to be reused. Additional work is needed to explore this.

Security and Usability Perceptions. When asked about the security perception of their chosen secret PIN, 83% of participants in both 4- and 6-digit PIN treatments felt their secret PIN was "secure" or "somewhat secure." In reality, 90% of PINs were unguessed, so participants were roughly correct in our threat model. For memorability, however, 97% of participants in the 4-digit PIN treatment perceived their PIN to be "memorable" or "somewhat memorable" compared to 90% in the 6-digit PIN treatment. Overall, while participants perceive both their 4- and 6-digit PINs to be secure, they find 4-digit PINs to be slightly more usable compared to 6-digit PINs. Given the unclear security benefits of longer PIN lengths, system designers should carefully consider the additional usability burdens of 6-digit PINs as well as their limited security improvement over 4-digit PINs before increasing PIN lengths.

Guessing Strategies. In contrast to the selection strategies for secret PINs, which have a large dependency on PIN length, guessing strategies for 4-digit and 6-digit PINs were mostly similar. While most participants selected their secret PINs using *dates* to make them *memorable*, they often went for *simple* PINs when guessing other participants' PINs (n = 39; 37% for 4-digit and n = 34; 32% for 6-digit). Rather than speculate on what dates or what sequences might be memorable to other users, most participants focused on simple PINs—even though participants themselves most often used dates to select their secret PINs. For instance, P2 noted: "I knew ii [*sic*] wouldn't be able to guess ones that were chosen because they were meaningful for some reason so I picked ones that are easy to type."

4.2 RQ2: Novice Attackers

In this section, we compare our new dataset with the data-driven guessers that have mostly been used in previous studies [30, 36, 53]. To our knowledge this is the first dataset of its kind in the literature.

Datasets. In Section 4.1, we analyzed the features of these PINs in our dataset and how they are selected. Now, we utilize them to study the guessing resistance of PINs in our threat model. Following the way participants were primed and their assigned PIN length (see Section 3), we refer to the datasets as *Secret-4*, *Secret-6*, *Guess-4*, and *Guess-6*.

Since PINs are usually stored and validated on individual devices instead of web servers, no large-scale leaks of PINs have yet appeared. Therefore, previous studies have relied on a bricolage of datasets that were collected outside the bounds of a controlled experiment, that we will call data-driven approaches. Our controlled experiment was motivated in part to evaluate the earlier datasets against our new experimental evidence. Probably the largest, although not collected within the bounds of a controlled experiment, is composed of 204 508 4-digit PINs. These PINs were gathered by the iOS application "Big Brother Camera Security" from Daniel

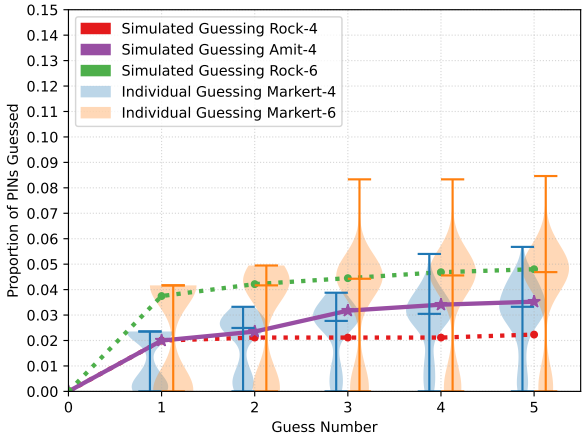


Figure 1: Individual guessing performance of participants' guesses as well as the simulated guessing performance of other datasets (Rock-4, Amit-4, Rock-6) when guessing Markert-4 and Markert-6.

Amitay [4]; we refer to this dataset as *Amit-4*. Since Amitay collected only 4-digit PINs, a similarly-sized 6-digit dataset is not available. Other datasets have been derived from leaked alphanumeric passwords. For instance, 4- and 6-digit subsequences were extracted from the RockYou password leak by Bonneau et al. [14] and Wang et al [53]. We refer to these datasets as *Rock-4* and *Rock-6*. Two datasets have also been collected within the bounds of a controlled experiment; Markert et al. collected both 4- and 6-digit PINs from participants primed to choose secret PINs [30] which we call *Markert-4* and *Markert-6*, respectively.

Individual Performance. We now examine participants' individual guessing performance, i.e., the smartphone-unlock guessing threat posed by novice everyday attackers. We focus on their performance in successfully guessing the secret PINs collected as part of this study but also datasets used in prior work. We additionally highlight trends that emerged from the guessability analysis for both 4- and 6-digit PINs.

The 1050 guesses we collect (525 for each PIN length) comprise a total of 415 distinct PINs. In the 4-digit case, we observed 177 different PINs (1.77% of all possible PINs), and 238 different 6-digit PINs (0.0238% of all possible PINs). Of these 415 PINs, 91% (378) were guesses of three or fewer participants, and only eight (2%) were guesses of more than 20 participants. Interestingly, these eight very popular guesses split evenly between the two lengths and follow similar patterns: the 4-digit PINs were `0000`, `1111`, `1234`, and `2580`, the 6-digit PINs were `000000`, `111111`, `123456`, and `987654`.

In terms of the guessing resilience of participants' secret PINs, the PINs of 21 participants (10%) were guessed (amounting to 16 unique PINs). Fourteen (13%) of these were 4-digit, 7 (7%) a 6-digit PIN. Regarding the variety of the selections, the 21 participants selected 16 different secret PINs, 10 of them being 4-digit PINs (`0000`, `1234`, `1478`, `1990`, `1995`, `1997`, `2000`, `2468`, `2580`, `6666`) and six 6-digit PINs (`121212`, `123456`, `134679`, `135790`, `159753`, `654321`). From the guessers' perspective, 179 participants (85%) guessed at least one secret PIN: (95; 91%) in the 4-digit and (84; 80%) in the

6-digit treatment. In prior work [30, 36, 53], the insecurity of 6-digit PINs arose from a stark selection bias, particularly with 123456 tending to be overwhelmingly popular. Among the Secret-6 PINs, we did not observe this shift. The reasons for this shift are unclear; while our study carefully reproduced the "look and feel" of prompts used in prior work, our priming of users may have caused more secure PIN choices.

The violin plots in Figure 1 show the range of individuals' PIN-guessing performance on a guess-by-guess basis when guessing the Markert-4 and Markert-6 dataset. For example, after one guess, the median, shown as a vertical line, for both 4- and 6-digit is equal to the maximum proportion guessed: 2% for 4-digit and 4% for 6-digit PINs. The median gains in individual performance after the first guess are marginal for both 4- and 6- digit PINs. The highest increase happens after the third guess for 6-digit PINs and the fourth guess for 4-digit PINs. For 4-digit PINs, the proportion guessed increases from 4% (3 guesses) to 5% (4 guesses), for 6-digit, from 5% (2 guesses) to 8% (3 guesses). Overall, novice guessers perform better at guessing 6-digit than 4-digit PINs in Markert et al.'s dataset, similar to previous findings about the success rate of data-driven attacks against 4- and 6-digit PINs chosen without explicit security focus [30, 53].

Combined Performance. To assess the performance of participants' guesses in aggregate, we combined all guesses to carry out a simulated attack against different 4- and 6-digit PIN datasets, following the approach in the previous work of Markert et al., Munyendo et al. [30, 36], and others. These prior works used leaked data to model attacker behavior. Our work gathers the first dataset of its kind: experimental data from participants primed to play the part of a guessing attacker. In this section, we will compare the guessing performance of our experimental-data model with the leaked data used in the prior work. This aggregated novice attacker is created based on the guessing order we derive from merging the five guesses of all participants into a single dataset. If two or more PINs share the same frequency in this dataset, we first try to rank them based on the order in which the participants guessed them. For example, if two PINs both occurred once but one of them was the third guess and other the fifth, we guess the third guess first because it had a higher "priority" for the participant.

An alternative approach sometimes seen in the guessing literature is to use the guesses from a study as a training set for a Probabilistic Context-Free Grammar (PCFG)- or Markov-based approach, following Wang et al. [54] that would generate many more guesses and therefore reach a strength estimation for the remaining (unguessed) PINs. A PCFG approach can be helpful when guessing variable-length passwords that follow a *system*, i.e., a generative structure like name followed by date. According to our participants, less than 5% used a system. But the contribution of our work is precisely to understand the actual guesses for 4- and 6-digit PINs directly observed in our study. Moreover, we aim for novice guessers who are strictly limited to a small handful of guess attempts. Developing a guessing order for the remaining unguessed PINs only applies to *unthrottled* attackers who could make hundreds or thousands of guesses. As this attacker could merely try all possible 4-digit or 6-digit PINs, they are outside our threat model.

Figure 2a shows the performance of participants' 4-digit guesses, while Figure 2b shows it for the 6-digit guesses. When considering 4-digit PINs, participants' guesses have a comparable effectiveness when guessing the *Rock-4* (●) and Markert-4 (+) datasets, but perform slightly better on other participants' *Secret-4* PINs (●). Interestingly, the success rate against *Amit-4* (★) is noticeably better, with over 15% of PINs in this dataset guessed after 20 guesses. This difference between the guessing performance of the *Amit-4* dataset compared to the remaining sets could be attributed to users not being primed for security during the selection of PINs in the Amitay app. This can be investigated in future research.

For 6-digit PINs, the success rate of participants' guesses is lower in guessing other participants' secret PINs (●) compared to PINs from the Markert-6 (+) dataset. However, the difference is even greater when guessing *Rock-6* PINs (●), attributed to the popularity of 123456 in *Rock-6*, leading to a substantial portion of PINs being guessed with just one guess. After this first guess, the success rate is more consistent with performance against the other two datasets.

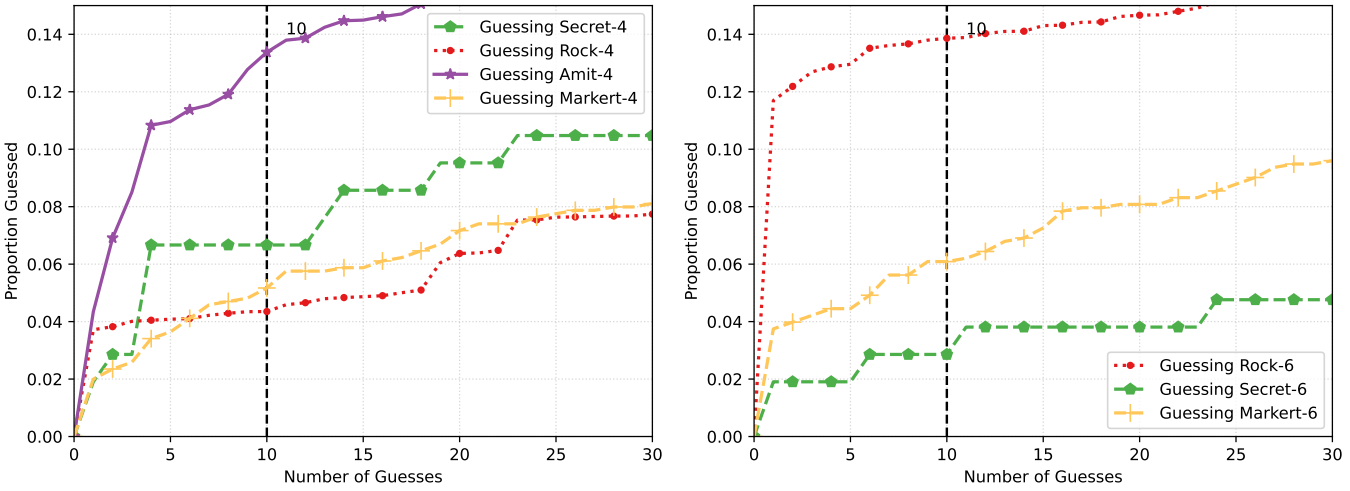
From Figure 2a and Figure 2b, we see that the participants' guesses perform similarly or better on previously published datasets compared to the secret PINs selected by participants, particularly for 6-digit PINs. As previously discussed in Section 4.2, there were only six different 6-digit secret PINs that were successfully guessed. This likely suggests that encouraging users to select secret PINs that cannot be easily guessed is a promising way to make them select more secure PINs. However, additional work is needed to specifically explore the exact messaging and implementation.

We show how well participants' guesses, secret PINs, and the Amitay and RockYou datasets perform when guessing PINs from Markert-4 (Figure 3a) and Markert-6 (Figure 3b). This serves as a benchmark to assess the effectiveness of participants' selections when applied to other datasets previously collected from the literature. Overall, participants' secret PINs (●) perform the worst of the datasets at guessing Markert-4 and by an even wider margin in the case of Markert-6. In the prior case, *Guess-4* (▲) performs similarly to *Amit-4* (★), while *Secret-4* performs comparably to *Rock-4* (●). However, in the case of Markert-6, the performance is more varied, with *Secret-6* (●) performing poorly, guessing only one PIN correctly. Conversely, *Guess-6* (▲) performs similarly to *Rock-6* (●) when guessing the Markert-6 dataset.

Overall, we find that the *Amit-4* dataset performs comparably to participants' *Guess-4* PINs, while the success rate of the *Rock-6* based attacker is similar to the *Guess-6* PINs of participants. This shows that on aggregate, novice attackers perform similarly to data-driven attackers, and thus supports the ecological validity of previous studies [30, 36, 53] that have used the Amitay dataset to guess 4-digit PINs, and RockYou to guess 6-digit PINs.

4.3 RQ3: Context for Smartphone Access

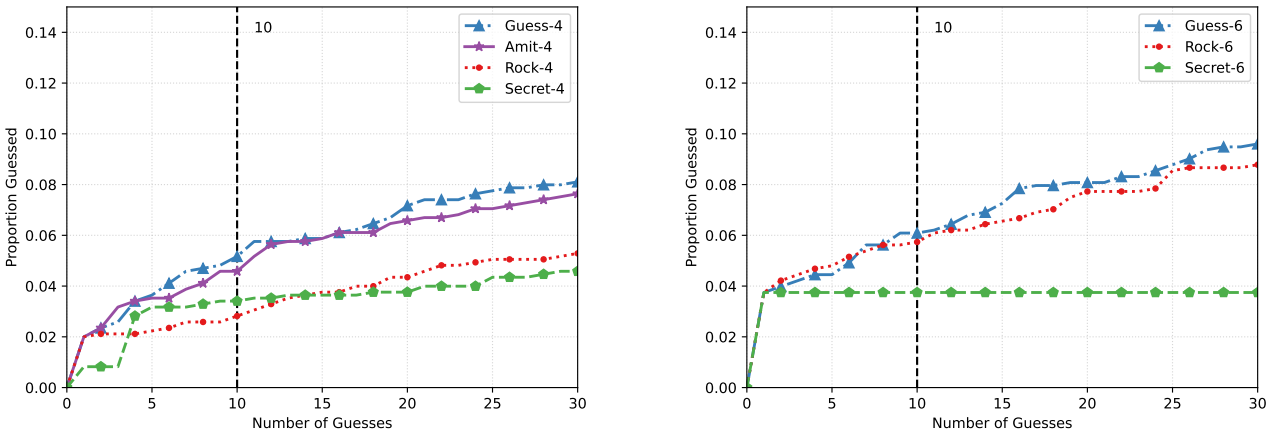
Delegation and Emergency Access. Previous work [25, 48] has shown that sharing behaviors are common with regard to smartphones, and that users have a desire to grant others limited, temporary access to their devices. In this section, we explore how these sharing and delegation behaviors align with the threat models envisioned by participants.



(a) Success rate of participants' 4-digit guesses.

(b) Success rate of participants' 6-digit guesses.

Figure 2: Success rate of the aggregated dataset based on participants' guessing PINs when attacking the aggregated dataset based on participants' secret PINs and other PIN datasets.



(a) Guessing Markert-4 dataset.

(b) Guessing Markert-6 dataset.

Figure 3: Using indicated datasets to guess 4- and 6-digit PIN datasets from Markert.

In Q9, we asked participants to "describe a situation where someone is most likely to unlock your smartphone." Answers overwhelmingly mention a close social contact, rather than a stranger or thief. The combined categories of *partner*, *friend*, and *family* account for 178 out of the total 210 responses (85%). In contrast, only seven participants (3%) mention a *thief* or *stranger*. Considering *partner*, the most-frequent code (81; 39%), P25 stated: "I can imagine my wife needing my PIN to access my phone to make a payment in a store and when my hands were full."

In spite of that, individuals in the partner category are not without risk. The prevalence of this category in our data combined with the work of Tseng et al. [49] on intimate partner surveillance points to a need to further understand the nuances of PIN security in controlling types of unauthorized access by insiders. Relationships within the *family* (50; 24%) or with a *friend* (47; 22%) have already been shown to pose similar risks [17, 44].

Subsequently, Q10 asked *why* the individual would access their phone. Most often, participants describe some form of *delegation* (88; 42%), with P37 saying: "They would just be looking at a text or notification to let me know what it said while I was presumably otherwise occupied."

Finding some information, not necessarily with a bad intent, was the second most popular answer (38; 18%). For example, P175 said the person might "check something like the weather or bus schedule." A similar use case, specifically in the form of someone borrowing the phone, was described by 21 participants (10%).

Many participants also identified a special category of delegation: they indicated that someone would access their smartphone in

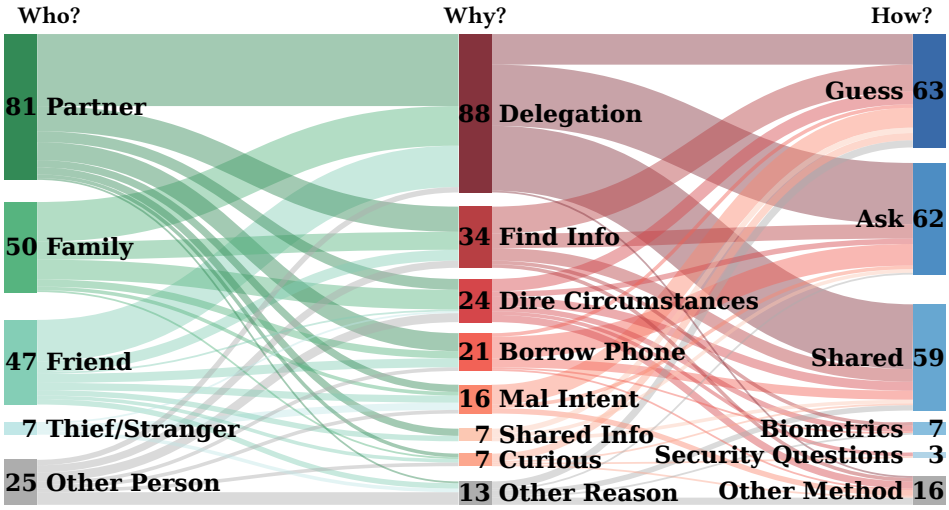


Figure 4: Participants' answers to Q9 asking *who* would try to access their smartphone, Q10 asking *why* this person would try to access it, and Q11 asking *how* this person would try to gain access.

dire circumstances (24; 11%), e.g., when the owner is physically incapacitated. P112 said "in case of an emergency he might be unlocking my phone to get help." While unlocking the phone to call for help is a valid scenario, sharing one's PIN for this purpose is not necessary as both Android and iOS allow anyone to make emergency calls even when the device is locked. System developers have also been improving features that can further assist with delegation and emergency access. For example, Android 13 allows user profiles to be switched on from the lock screen and guest users granted access to installed apps [23] and Android 14 may allow "cloned apps" to permit multiple installations of a given app to use different user profiles [40]. This development suggests a broader recognition in the industry of this user concern and would give added prominence to the feature of user profiles. In our study, *no* participants mentioned user profiles despite the preponderance of scenarios where profiles would be of benefit, suggesting the need for more user education and awareness about this feature.

There appears to be a prevalence of benign motivations from close social contacts when it comes to accessing participants' phones (see Figure 4). This might come from the social-desirability bias which might have made participants hesitate to be forthcoming about malicious activity in response to this question. On the other hand, more than 37% admitted to "trying to access someone else's smartphone without their knowledge" in Q17, which is more than those who mentioned *mal-intent* (16; 8%) in Q10. Moreover, this finding is comparable to the 39% found by Marques et al [32].

Participants also provided responses to Q11 asking about "the strategy the individual would use to gain access to your smartphone." Although guessing was the most prominent answer, responses continued with the general theme of benign access by social contacts. More than half of participant responses indicated that the person would simply *ask* (62; 30%) or already know the PIN because it is *shared* (59; 28%). P15 said "I would tell them the code," while P79 added: "He knows my PIN... but my trick is to say 'it's my birthday' which shows me who knows when my birthday is!"

This willingness to allow others access was further confirmed by the responses to Q18. A large majority (184; 88%) said they have granted someone else access before, while (23; 11%) had not.

Controlling Access and Guessing. We found that participants had difficulty controlling access, with nearly half (95; 45.2 %) reporting that they had changed their PIN specifically to prevent someone's access in Q16. As guessing is the main focus of our study, we additionally reviewed all responses to Q11 that mention guessing. By this more-inclusive measure, 78 responses were included in this additional analysis.

A total of 51 responses mentioned the use of personal knowledge in formulating guesses. As an example, P86 said "she would use my date of birth, or she would use the ages of my grandkids." This finding suggests an opportunity for future work focusing on guessers who incorporate personal knowledge and is echoed by Munyendo et al. [36] who found a personal hint can be effective in helping predict someone's PIN. In contrast, comparatively fewer participants (12; 15 %) reported shoulder-surfing in their scenario. Previous work such as from Aviv et al. [10] suggest that only about 11 % of shoulder-surfing attacks on 6-digit PINs are successful. For comparison, of the 51 responses who mentioned personal hints, there were (33; 65 %) occurrences of *birthday, day,* or *date.* This confirms prior work [14, 36] that has similarly shown that personal hints including birthdays can reveal users' PINs.

Q14 and Q15 specifically asked about participants' level of concern about their phone being accessed *without* their consent. About half of participants were "somewhat concerned" (67; 32%) or "concerned" (26; 12%), with most of them saying that they keep sensitive information on their phone. Except for 8% who were indecisive, all others indicated they were "somewhat unconcerned" (53; 25%) or "unconcerned" (47; 22%). Most of these do not believe their phone can be unlocked by someone else while others trust their surroundings or believe they have nothing to hide.

To investigate participants' perception about the security of their secret PIN, Q19 asked if they think their secret PIN will be guessed by other participants. Most participants said no (138; 66%), and only five of them were wrong. The PINs they picked were years (`1990`, `2000`) or common schemes (`2580`, `6666`, `121212`). In contrast, of those who believed their PIN would be guessed (71; 34%), 16 were right. In other words, there was a tendency across participants to underestimate the security of their PIN.

Finally, Q20 asked "Do you think you guessed someone else's secret PIN? Why or why not?" Most participants said yes or maybe (164; 78%), with a majority (134; 82%) of them right. On the other hand, (43; 20%) said they would not guess correctly: of these, only (14; 33%) were right. Participants who thought they did not guess the PIN of another participant mostly mentioned that the PIN would be of *personal importance* to a stranger or *random*. Participants who thought they did guess correctly indicated that other participants artificially *picked easy PINs*, e.g., P112 was right in saying: "I think I guessed someones PIN. Someone definitely used 0000."

Participant Misconceptions. We were particularly interested in the survey responses of the 21 whose PINs were guessed by another participant. Nine mentioned having important information or valuing their privacy while only four mentioned some variation on trusting others or having nothing to hide. When asked how someone would access their phone, only four mentioned guessing compared to 10 who said the person would ask. Five participants chose a PIN that was *simple*, while another five chose a PIN that was *memorable*.

Of the 21, only seven thought their secret PIN would be guessed by another participant, suggesting that most participants were not purposefully setting weak PINs. The 14 participants who were overconfident highlight an opportunity for user education, as three said their PIN was reused while another three said their PIN was random.

5 DISCUSSION AND CONCLUSION

Any reasonable definition of a secure PIN is that it must resist some form of guessing. Exactly how much guessing is subject to interpretation, both by experts — and clearly by users. In this paper, we analyze the guessability and threat models of human-chosen 4- and 6-digit PINs for smartphone unlock by considering more commonplace novice attackers. Overall, we find that novice guessers perform comparably to the data-driven attackers employed in prior work [30, 36, 53], that a third of participants recently tried to access someone else's smartphone without their knowledge, that people mostly are concerned about their close social connections, perhaps underestimating theft or loss, and that most people would like to delegate access to their smartphones in some way. In the rest of this section, we discuss these findings further and offer recommendations to system designers that can improve the security of human-chosen PINs.

Modeling Novice PIN Guessers. With the setup of our study, each secret PIN is subjected to five guesses from the remaining 104 participants in that treatment. Where Roberts et al. [43] illustrate the payoff in terms of accessible data, we focus here on the guessing attack. For instance, they report a guess-success rate of 4.8% overall, but using a mix of authentication types (patterns, PINs, others). We focus on this attack model as user-chosen PINs can be subjected to potentially many guessing attempts over their lifetime. For instance, in their study, Harbach et al. [24] found that only 7.3% of participants changed their PIN *even after they suspected someone was looking over their shoulder*. Similarly, PINs are frequently reused. We found the reuse effect to be so pronounced that (58; 27%) of participants said they gave their actual smartphone (or other personal device) unlock PIN as their secret PIN in the study, even though we instructed them not to do so. Further, a user's PIN may persist for years across device replacement cycles, and will inevitably present opportunities where novice strangers or close friends may try to unlock and gain access to the device. Our data shows that 77 (37%) participants admit to having tried to unlock someone else's smartphone without their knowledge, indicating that a PIN may be subjected to many guessing attempts. Moreover, (95; 45%) of participants changed their PIN to keep someone from accessing their phone, an indication that users take the threat of PIN-guessing seriously.

New Dataset. Our new dataset provides important experimental support for the simulated attacking routines used in previous studies. The direct comparison is shown in the median performance in Figure 1. Our results also show that the guessing risk appears concentrated in a small number of common PINs, for example 0000. The fact that some participants chose these as their PIN (with only one-third of these saying it was likely it would be guessed) highlights something of a misunderstanding of which PINs are commonly guessed. Further, given (71; 34%) of participants thought their PIN would be guessed and only (16; 23%) were correct, many participants are *overestimating* the vulnerability of human-chosen PINs to novice guessing strategies. Therefore, design interventions should be *targeted* so that users can respectively modify selection behaviors, or gain confidence in the strength of their choices.

Implications for System Designers. Previous work has shown how to build optimized blocklists [30] from data-driven attackers. Here, we find a justification for a small additional blocklist consisting of those PINs guessed in our study. These PINs that were guessed tended to be guessed by many participants, meaning the novice guessing risk is concentrated in a small number of PINs. Therefore, systems could introduce additional friction for the user based on our results. Messaging to users could take on additional urgency, such as "This PIN would be guessed by *many* people." In addition, though the iOS blocklist currently allows a user to select "Use Anyway," the risk posed suggests these guessed PINs to be completely disallowed. There is, as ever, an opportunity for user education shown by the fact that only one-third of participants whose PIN was guessed believed this would be true. Our work agrees with Marques et al. [31] who suggested adding some realistic details when explaining attacks to users, emphasizing the aspects of unattended access by non-strangers. As an example, Marques et al. dub this the *shower-time attack*, to emphasize threats from non-strangers with low technical skills and only a short time to act. The fact that "safe" physical spaces may sometimes allow unattended access attempts by insiders has been previously encapsulated in the phrases *lunchtime* or *midnight* attacks, noted by Naor and Yung to be "folklore" as early as 1990 [38]. Future work could test which,

if any, of these phrases might lead to changes in user behavior. Finally, users could be notified when unsuccessful guessing occurs on their device. It is by now common for websites to send emails when the site is accessed by a new device or in a new location. The device could send an email to the owner when a PIN is guessed incorrectly. This approach would make this attack less surreptitious and perhaps discourage attackers.

PIN Length. In our attack setting where novice individuals provide five guesses applied to 104 simulated smartphones, participants performed better against 4-digit PINs than 6-digit PINs; nearly twice as many 4-digit PINs (14; 13%) compared to (7; 7%) of 6-digit PINs were guessed. However, when using our participants' guesses to target a larger dataset such as the one collected by Markert et al. [30], we find that 6-digit PINs are more easily guessed compared to 4-digit PINs, matching prior work [30, 36, 53] that have similarly shown that 6-digit PINs offer limited security improvements over 4-digit PINs. Nonetheless, encouraging users to select secure PINs, of either 4- or 6-digit, might have better security outcomes than simply asking users to upgrade to 6-digit PINs, as noted by Munyendo et al [36].

Users' Perceived Threat Models. When asked about scenarios in which someone would actually access their smartphone, participants overwhelmingly mentioned close social contacts. Most common was a desire to *delegate* some forms of access to the device for example when driving. Others in the literature such as Karlson et al. [25] have similarly observed that users express a desire for delegated or guest accounts. Our survey also found that participants had some difficulty controlling this access, with nearly half reporting that they had changed their PIN specifically to prevent someone's access. Android 13 revamps the user-profile feature making it easier to delegate access. Given that no participants in our study mentioned user profiles, there is a need for more user awareness and education on this improved feature, as well as how users can use it. Further, participants mostly do not consider (and report being generally unconcerned about) scenarios of malintent by strangers when selecting either their "secret PIN" or their guesses, suggesting they value an easily-remembered PIN over guessing resistance. More than half of respondents who mentioned guessing in their scenario said the person would use a personal hint. More than half of those mentioned "day," "date," or "birthday" suggesting an opportunity for future work to better understand the resistance of PINs to guessing in the presence of hints or other personal or additional information.

ACKNOWLEDGMENTS

We thank all the anonymous reviewers for their insightful comments and feedback. This material is based upon work supported by the National Science Foundation under Grant No. 1845300.

REFERENCES

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-Based User Authentication. In *ACM Conference on Human Factors in Computing Systems (CHI '17)*. ACM, Denver, Colorado, USA, 3751–3763.

[2] Elham Al Qahtani, Mohamed Shehab, and Abrar Aljohani. 2018. The Effectiveness of Fear Appeals in Increasing Smartphone Locking Behavior Among Saudi Arabians. In *Symposium on Usable Privacy and Security (SOUPS '18)*. USENIX, Baltimore, Maryland, USA, 31–46.

[3] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. 2017. "...better to use a lock screen than to worry about saving a few seconds of time": Effect of Fear Appeal in the Context of Smartphone Locking Behavior. In *Symposium on Usable Privacy and Security (SOUPS '17)*. USENIX, Santa Clara, California, USA, 49–63.

[4] Daniel Amitay. 2011. Most Common iPhone Passcodes. http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes, as of September 24, 2023.

[5] Panagiotis Andriotis, Theo Tryfonas, and George Oikonomou. 2014. Complexity Metrics and User Strength Perceptions of the Pattern-Lock Graphical Authentication Method. In *Conference on Human Aspects of Information Security, Privacy and Trust (HAS '14)*. Springer, Heraklion, Crete, Greece, 115–126.

[6] Panagiotis Andriotis, Theo Tryfonas, George Oikonomou, and Can Yildiz. 2013. A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '13)*. ACM, Budapest, Hungary, 1–6.

[7] Android Open Source Project. 2021. Android 13: GateKeeper – ComputeRetryTimeout Function. https://android.googlesource.com/platform/system/gatekeeper/+/refs/heads/android13-release/gatekeeper.cpp#282, as of September 24, 2023.

[8] Apple. 2015. iOS 9 Preview. https://web.archive.org/web/20150608223846/http://www.apple.com/ios/ios9-preview/, as of June 8, 2015.

[9] Adam J. Aviv, Devon Budzitowski, and Ravi Kuber. 2015. Is Bigger Better? Comparing User-Generated Passwords on 3x3 vs. 4x4 Grid Sizes for Android's Pattern Unlock. In *Annual Computer Security Applications Conference (ACSAC '15)*. ACM, Los Angeles, California, USA, 301–310.

[10] Adam J. Aviv, John T. Davin, Flynn Wolf, and Ravi Kuber. 2017. Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Annual Conference on Computer Security Applications (ACSAC '17)*. ACM, Orlando, Florida, USA, 486–498.

[11] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *USENIX Workshop on Offensive Technologies (WOOT '10)*. USENIX, Washington, District of Columbia, USA, 1–7.

[12] Adam J. Aviv, Flynn Wolf, and Ravi Kuber. 2018. Comparing Video Based Shoulder Surfing with Live Simulation and Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Annual Conference on Computer Security Applications (ACSAC '18)*. ACM, San Juan, Puerto Rico, USA, 453–466.

[13] Daniel V. Bailey, Philipp Markert, and Adam J. Aviv. 2021. "I have no idea what they're trying to accomplish:" Enthusiastic and Casual Signal Users' Understanding of Signal PINs. In *Symposium on Usable Privacy and Security (SOUPS '21)*. USENIX, Virtual Conference, 417–436.

[14] Joseph Bonneau, Sören Preibusch, and Ross Anderson. 2012. A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs. In *Financial Cryptography and Data Security (FC '12)*. Springer, Kralendijk, Bonaire, 25–40.

[15] Maria Casimiro, Joe Segel, Lewei Li, Yigeng Wang, and Lorrie Faith Cranor. 2020. A Quest for Inspiration: How Users Create and Reuse PINs. In *Who Are You?! Adventures in Authentication Workshop (WAY '20)*. Virtual Conference, 1–7.

[16] Seunghun Cha, Sungsu Kwag, Hyoungshick Kim, and Jun Ho Huh. 2017. Boosting the Guessing Attack Performance on Android Lock Patterns with Smudge Attacks. In *ACM Asia Conference on Computer and Communications Security (ASIA CCS '17)*. ACM, Abu Dhabi, United Arab Emirates, 313–326.

[17] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and Teens' Perspectives on Privacy In a Technology-Filled World. In *Symposium on Usable Privacy and Security (SOUPS '14)*. USENIX, Menlo Park, California, USA, 19–35.

[18] 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 *ACM Conference on Human Factors in Computing Systems (CHI '14)*. ACM, Toronto, Ontario, Canada, 2937–2946.

[19] 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 *ACM Conference on Human Factors in Computing Systems (CHI '17)*. ACM, Denver, Colorado, USA, 4254–4265.

[20] Cyrus Farivar. 2015. Apple to Require 6-digit Passcodes on Newer iPhones, iPads Under iOS 9. https://arstechnica.com/?post_type=post&p=679147, as of September 24, 2023.

[21] Federal Communications Commission. 2018. Technological Advisory Council (TAC) Mobile Device Theft Prevention (MDTP) Working Group. https://transition.fcc.gov/bureaus/oet/tac/tacdocs/reports/2018/11.30.18-MDTP-WG-Report-and-Recommendations.pdf.

[22] Federal Trade Commission. 2022. How to Protect Your Phone from Hackers. https://consumer.ftc.gov/articles/how-protect-your-phone-hackers.

[23] Google Developers. 2022. Android 13 Developer Preview. https://developer.android.com/about/versions/13, as of September 24, 2023.

[24] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a Hard Lock Life: A Field Study of Smartphone

(Un)Locking Behavior and Risk Perception. In *Symposium on Usable Privacy and Security (SOUPS '14)*. USENIX, Menlo Park, California, USA, 213–230.
[25] Amy K. Karlson, A.J. Bernheim Brush, and Stuart Schechter. 2009. Can I Borrow Your Phone? Understanding Concerns When Sharing Mobile Phones. In *ACM Conference on Human Factors in Computing Systems (CHI '09)*. ACM, Boston, Massachusetts, USA, 1647–1650.
[26] 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 '20)*. ACM, Austin, Texas, USA, 249–262.
[27] Lydia Kraus, Tobias Fiebig, Viktor Miruchna, Sebastian Möller, and Asaf Shabtai. 2015. Analyzing End-Users' Knowledge and Feelings Surrounding Smartphone Security and Privacy. In *Mobile Security Technologies (MoST '15)*. San Jose, California, USA.
[28] Marte Løge, Markus Dürmuth, and Lillian Røstad. 2016. On User Choice for Android Unlock Patterns. In *European Workshop on Usable Security (EuroUSEC '16)*. ISOC, Darmstadt, Germany.
[29] Ahmed Mahfouzab, Ildar Muslukhova, and Konstantin Beznosova. 2016. Android Users in the Wild: Their Authentication and Usage Behavior. *Pervasive and Mobile Computing* 32 (Oct. 2016), 50–61.
[30] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. 2021. On the Security of Smartphone Unlock PINs. *ACM Transactions on Privacy and Security* 24, 4 (Nov. 2021), 30:1–30:36.
[31] Diogo Marques, Tiago Guerreiro, Luis Carriço, Ivan Beschastnikh, and Konstantin Beznosov. 2019. Vulnerability & Blame: Making Sense of Unauthorized Access to Smartphones. In *ACM Conference on Human Factors in Computing Systems (CHI '19)*. ACM, Glasgow, Scotland, United Kingdom, 589:1–589:13.
[32] Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. 2016. Snooping on Mobile Phones: Prevalence and Trends. In *Symposium on Usable Privacy and Security (SOUPS '16)*. USENIX, Denver, Colorado, USA, 159–174.
[33] Matthews, Tara and Liao, Kerwell and Turner, Anna and Berkovich, Marianne and Reeder, Rob and Consolvo, Sunny. 2016. "She'll just grab any device that's closer": A Study of Everyday Device & Account Sharing in Households. In *ACM Conference on Human Factors in Computing Systems (CHI '16)*. ACM, San Jose, California, USA, 5921–5932.
[34] William Melicher, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L. Mazurek. 2016. Usability and Security of Text Passwords on Mobile Devices. In *ACM Conference on Human Factors in Computing Systems (CHI '16)*. ACM, San Jose, California, USA, 527–539.
[35] Collins W. Munyendo, Miles Grant, Philipp Markert, Timothy J. Forman, and Adam J. Aviv. 2021. Using a Blocklist to Improve the Security of User Selection of Android Patterns. In *Symposium on Usable Privacy and Security (SOUPS '21)*. USENIX, Virtual Conference, 37–56.
[36] Collins W. Munyendo, Philipp Markert, Alexandra Nisenoff, Miles Grant, Elena Korkes, Blase Ur, and Adam J. Aviv. 2022. "The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 Digits. In *USENIX Security Symposium (SSYM '22)*. USENIX, Boston, Massachusetts, USA.
[37] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. 2013. Know Your Enemy: The Risk of Unauthorized Access in Smartphones by Insiders. In *Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '13)*. ACM, Munich, Germany, 271–280.
[38] Moni Naor and Moti Yung. 1990. Public-key Cryptosystems Provably Secure against Chosen Ciphertext Attacks. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA*, Harriet Ortiz (Ed.). ACM, 427–437.
[39] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. 2017. Beyond the Turk: Alternative Platforms for Crowdsourcing Behavioral Research. *Journal of Experimental Social Psychology* 70, 5 (May 2017), 153–163.
[40] Mishaal Rahman. 2023. Android 14 Could Let You Clone Apps. https://www.xda-developers.com/android-14-app-cloning/, as of September 24, 2023.
[41] Elissa M. Redmiles, Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek. 2017. *A Summary of Survey Methodology Best Practices for Security and Privacy Researchers*. Technical Report CS-TR-5055. UM Computer Science Department.
[42] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2019. How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples. In *IEEE Symposium on Security and Privacy (SP '19)*. IEEE, San Francisco, California, USA, 227–244.
[43] Richard Roberts, Julio Poveda, Raley Roberts, and Dave Levin. 2023. Blue Is the New Black (Market): Privacy Leaks and Re-Victimization from Police-Auctioned Cellphones. In *IEEE Symposium on Security and Privacy (SP '23)*. IEEE, San Francisco, California, USA.
[44] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Symposium on Usable Privacy and Security (SOUPS '18)*. USENIX, Baltimore, Maryland, USA, 127–142.
[45] Raina Samuel, Philipp Markert, Adam J. Aviv, and Iulian Neamtiu. 2020. Knock, Knock. Who's There? On the Security of LG's Knock Codes. In *Symposium on Usable Privacy and Security (SOUPS '20)*. ACM, Virtual Conference, 37–59.
[46] Florian Schaub, Ruben Deyhle, and Michael Weber. 2012. Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms. In *International Conference on Mobile and Ubiquitous Multimedia (MUM '12)*. ACM, Ulm, Germany, 13:1–13:10.
[47] Elaine Shi, Yuan Niu, Markus Jakobsson, and Richard Chow. 2010. Implicit Authentication Through Learning User Behavior. In *International Conference on Information Security (ISC '10)*. Springer, Boca Raton, Florida, USA, 99–113.
[48] Frank Stajano. 2004. One User, Many Hats; and, Sometimes, No Hat: Towards a Secure Yet Usable PDA. In *International Conference on Security Protocols (SP '04)*. Springer, Cambridge, United Kingdom, 51–64.
[49] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2020. The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums. In *USENIX Security Symposium (SSYM '20)*. USENIX, Virtual Conference, 1893–1909.
[50] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. 2013. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. In *ACM Conference on Computer and Communications Security (CCS '13)*. ACM, Berlin, Germany, 161–172.
[51] Blase Ur, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Saranga Komanduri, Darya Kurilova, Michelle L. Mazurek, William Melicher, and Richard Shay. 2015. Measuring Real-World Accuracies and Biases in Modeling Password Guessability. In *USENIX Security Symposium (USENIX Security 15)*. USENIX, Washington, District of Columbia, USA, 463–481.
[52] Emanuel von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. 2015. Easy to Draw, but Hard to Trace?: On the Observability of Grid-based (Un)Lock Patterns. In *ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, Seoul, Republic of Korea, 2339–2342.
[53] Ding Wang, Qianchen Gu, Xinyi Huang, and Ping Wang. 2017. Understanding Human-Chosen PINs: Characteristics, Distribution and Security. In *ACM Asia Conference on Computer and Communications Security (ASIA CCS '17)*. ACM, Abu Dhabi, United Arab Emirates, 372–385.
[54] Ding Wang, Ping Wang, Debiao He, and Yuan Tian. 2019. Birthday, Name and Bifacial-Security: Understanding Passwords of Chinese Web Users. In *28th USENIX security symposium (USENIX security 19)*. Usenix, Santa Clara, CA, 1537–1555.
[55] Ding Wang, Zijian Zhang, Ping Wang, Jeff Yan, and Xinyi Huang. 2016. Targeted Online Password Guessing: An Underestimated Threat. In *ACM Conference on Computer and Communications Security (CCS '16)*. ACM, Vienna, Austria, 1242–1254.
[56] Oliver Wiese and Volker Roth. 2016. See You Next Time: A Model for Modern Shoulder Surfers. In *Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '16)*. ACM, Florence, Italy, 453–464.
[57] Almos Zarandy, Ilia Shumailov, and Ross Anderson. 2020. Hey Alexa What Did I Just Type? Decoding Smartphone Sounds With a Voice Assistant. *CoRR* abs/2012.00687 (Dec. 2020), 1–18.

APPENDIX

A SURVEY INSTRUMENT

Agenda

PINs or passcodes are often used to unlock mobile devices. You will be asked to choose a PIN just like you would to protect your smartphone. Afterward, you will complete a short survey and then try to guess the PINs of other participants. You will enter 5 guesses. Finally, you will answer some questions about your experience.

You contribute to research, so please answer correctly and as detailed as possible. Next, you will practice the PIN selection.

Practice entering a [4/6]-digit PIN.

PIN pad as shown in Figure 5

Your Task

You will be asked to choose a digit PIN you would use to unlock your smartphone. You will need to remember your secret PIN for the duration of the study. Please DO NOT write down your secret PIN.

Create a [4/6]-digit secret PIN

A secret PIN protects your data and is used to unlock your smartphone.

PIN pad as shown in Figure 5

Questionnaire

People use different strategies for choosing their PINs. Below, we will ask about your strategy.

Q1 What was your strategy for choosing your secret PIN?
Answer: _____

Please select the answer choice that most closely matches how you feel about the following statements:

Q2 I feel the secret PIN I chose is:
○ Secure ○ Somewhat secure ○ Neither secure nor insecure ○ Somewhat insecure ○ Insecure

Q3 I feel the secret PIN I chose is:
○ Easy to enter ○ Somewhat easy to enter ○ Neither easy nor hard to enter ○ Somewhat hard to enter ○ Hard to enter

Q4 I feel the secret PIN I chose is:
○ Easy to remember ○ Somewhat easy to remember ○ Neither easy nor hard to remember ○ Somewhat hard to remember ○ Hard to remember

Q5 What is the shape of a red ball?
○ Red ○ Blue ○ Square ○ Round

Q6 Was the secret PIN that you entered a PIN that you use on your smartphone or other personal devices?
○ Yes ○ No ○ Unsure ○ I do not lock my smartphone with a PIN

If participants indicated reuse of their PIN in Q6:

Q7 Did you choose a secret PIN you use in other contexts besides unlocking your smartphone? (Select all that apply)
□ ATM/Credit/Payment Card □ Laptop/PC □ Online Accounts □ Bike/Gym lock □ Electronic Door Lock □ Home Security System/Safe
□ Garage Door Opener □ Car/Truck/SUV □ Voicemail □ Gaming Console □ Smartwatch □ Other, please specify:
□ No, I did not choose a PIN from other contexts.

Your Task

- Enter 5 PINs that you think other participants entered
- Any number of correct guesses earns a bonus $0.50, paid 1-2 weeks after the completion of this study
- More than 100 people will be taking this study

Please enter 5 different guesses.

The following page appeared 5 times

Guess x

Try to guess someone's [4/6]-digit secret PIN. Guesses must be unique!

PIN pad as shown in Figure 7

About Your Guesses

Previously, you made the following guesses:
Guess 1: [pin]
Guess 2: [pin]
Guess 3: [pin]
Guess 4: [pin]
Guess 5: [pin]

Q8 In two to three sentences, please describe your overall strategy you used when guessing other participants' secret PINs.
Answer: _____

Q9 Please describe a situation where someone is most likely to unlock your smartphone. If relevant, indicate your relationship to this person but do NOT include Personally Identifiable Information (PII).
Answer: _____

Q10 In this situation, why would the individual be accessing your smartphone?
Answer: _____

Q11 In this situation, describe the strategy the individual would use to gain access to your smartphone.
Answer: _____

Q12 Did you consider this situation when you chose your secret PIN?
○ Yes ○ No ○ Unsure

Q13 Did you consider this situation when you were guessing the PINs of other participants?
○ Yes ○ No ○ Unsure

Q14 My level of concern for someone accessing my phone without consent is:
○ Unconcerned ○ Somewhat unconcerned ○ Neither concerned nor unconcerned ○ Somewhat concerned ○ Concerned

Q15 Why do you feel this level of concern?
Answer: _____

Q16 Have you ever changed your PIN to keep someone from accessing your smartphone?
○ Yes ○ No ○ Unsure

Q17 Have you ever tried to access someone else's smartphone without their knowledge?
○ Yes ○ No ○ Unsure

Q18 Have you ever granted someone else access to your smartphone?
○ Yes ○ No ○ Unsure

Re-enter your [4/6]-digit PIN

PIN pad as shown in Figure 5

About Your Guesses

Q19 Do you think the secret PIN you entered at the start of this survey will be guessed by other participants in this study? Why or why not?
Answer: _____

Q20 Do you think you guessed someone else's secret PIN? Why or why not?
Answer: _____

Enter Demographic Information

D1 What is your age range?
○ 18–24 ○ 25–34 ○ 35–44 ○ 45–54 ○ 55–64 ○ 65–74 ○ 75 or older ○ Prefer not to say

D2 What is your gender?
○ Woman ○ Man ○ Non-binary ○ Prefer to self-describe ○ Prefer not to say

D3 What is the highest degree or level of school you have completed?
○ Some high school ○ High school ○ Some college ○ Trade, technical, or vocational training ○ Associate's Degree ○ Bachelor's Degree ○ Master's Degree ○ Professional Degree ○ Doctorate ○ Prefer not to say

D4 Do you use any of the following biometrics to unlock your primary smartphone? (Select all that apply)
□ Fingerprint □ Face □ Iris □ Other biometric □ Prefer not to say

*If participants indicated **not** to use a biometric in D5:*

D5a How do you unlock your smartphone, if your biometric fails or when you reboot your primary smartphone?
○ None ○ Pattern ○ 4-digit PIN ○ 6-digit PIN ○ PIN of other length ○ Alphanumeric password ○ I use an unlock method not listed here ○ Prefer not to say

*If participants indicated **not** to use a biometric in D5:*

D5b What screen lock do you use to unlock your primary smartphone?
○ None ○ Pattern ○ 4-digit PIN ○ 6-digit PIN ○ PIN of other length ○ Alphanumeric password ○ I use an unlock method not listed here ○ Prefer not to say

D6 What is the operating system of your primary smartphone?
○ Android ○ iOS (iPhone) ○ Other ○ Prefer not to say

D7 Which of the following best describes your educational background or job field?
○ I have an education in, or work in, the field of computer science, computer engineering, or IT.
○ I do not have an education in, nor do I work in, the field of computer science, computer engineering, or IT.
○ Prefer not to say

One More Thing

Please indicate if you've honestly participated in this survey and followed instructions completely. You will not be penalized/rejected for indicating 'No' but your data may not be included in the analysis:
○ Yes ○ No

B DEMOGRAPHICS

Table 2: Demographic information of participants.

	Woman		Man		Non-Binary		Total	
	No.	%	No.	%	No.	%	No.	%
Age	112	53	90	43	8	4	210	100
18–24	46	22	20	10	5	2	71	34
25–34	41	20	40	19	1	0	82	39
35–44	17	8	21	10	2	1	40	19
45–54	7	3	7	3	0	0	14	7
55–64	1	0	1	0	0	0	2	1
65–74	0	0	0	0	0	0	0	0
75+	0	0	1	0	0	0	1	0
Prefer not to say	0	0	0	0	0	0	0	0
Education	112	53	90	43	8	4	210	100
Some High School	0	0	1	0	0	0	1	0
High School	0	0	1	0	0	0	1	0
Some College	20	10	11	5	2	1	33	16
Trade	24	11	14	7	3	1	41	20
Associate's	2	1	2	1	0	0	4	2
Bachelor's	11	5	3	1	0	0	14	7
Master's	40	19	42	20	2	1	84	40
Professional	11	5	9	4	1	0	21	10
Doctorate	2	1	3	1	0	0	5	2
Prefer not to say	2	1	4	2	0	0	6	3
Background	112	53	90	43	8	4	210	100
Technical	24	11	35	17	1	0	60	29
Non-Technical	85	40	52	25	6	3	143	68
Prefer not to say	3	1	3	1	1	0	7	3

C PIN FEATURES

Table 3: Features of the secret PINs and guesses. Note, some PINs, e.g., `0101` can match multiple categories, including *date* and *repeat*.

Secret PINs						Guesses					
4-digit			6-digit			4-digit			6-digit		
Date											
mmyy	27	26%	mmddyy	31	30%	mmyy	172	33%	mmddyy	83	16%
mmdd	21	20%	yymmdd	16	15%	mmdd	64	12%	yymmdd	55	11%
yyyy	11	11%	ddmmyy	14	13%	ddmm	51	10%	ddmmyy	46	9%
ddmm	9	9%	mmyyyy	4	4%	yyyy	24	5%	mmyyyy	9	2%
total	41	39%	total	34	32%	total	198	38%	total	86	16%
Repeat											
couplet	12	11%	couplet	7	7%	abab	141	27%	ababab	97	19%
triplet	4	4%	ababab	6	6%	couplet	126	24%	couplet	92	18%
abba	4	4%	aabbcc	2	2%	triplet	121	23%	triplet	85	16%
abab	3	3%	triplet	1	1%	abba	121	23%	aabbcc	78	15%
aaaa	2	2%				aabb	120	23%	abcabc	77	15%
aabb	2	2%				aaaa	119	23%	aaaaax	77	15%
									xaaaaa	76	15%
									aaaaaa	74	14%
total	15	14%	total	13	12%	total	150	29%	total	120	23%
Sequential											
asc	2	2%	asc	2	2%	asc	100	19%	asc	95	18%
asc even	1	1%	asc odd	1	1%	desc	36	7%	desc	40	8%
asc odd	1	1%	desc	1	1%	asc even	6	1%	asc odd	8	2%
			double-asc	1	1%	asc odd	5	1%	asc even	7	1%
									double-asc	4	1%
total	4	4%	total	5	5%	total	147	28%	total	154	29%
Walk											
vertical	8	8%	rectangle	5	5%	vertical	47	9%	rectangle	173	33%
diamond	2	2%	vertical	1	1%	corners	27	5%	horizontal	8	2%
diagonal	2	2%				diamond	12	2%	vertical	5	1%
corners	2	2%				rectangle	7	1%	corners	3	1%
rectangle	1	1%				box	6	1%	box	1	1%
horizontal	1	1%				diagonal	5	1%			
total	16	15%	total	6	6%	total	104	20%	total	190	36%
Total											
total	105		total	105		total	525		total	525	

D STUDY SCREENSHOTS

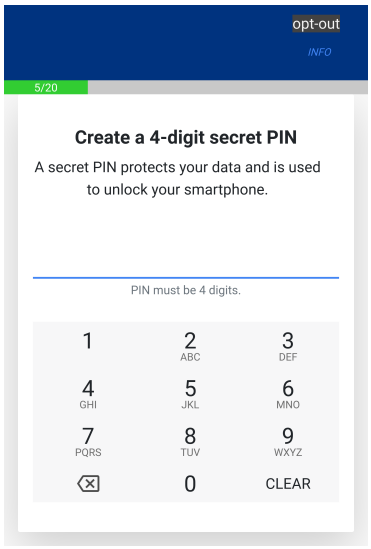


Figure 5: The page on which we asked the participants to create a 4- or 6-digit secret PIN.

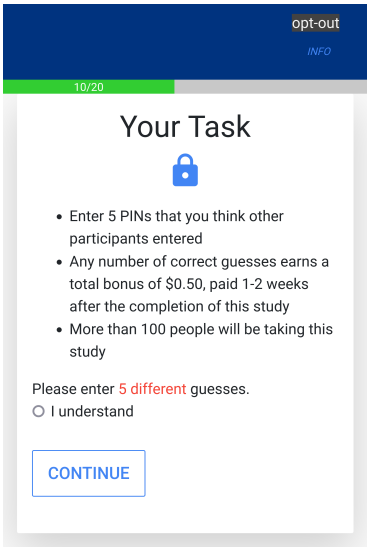


Figure 6: The instructions provided before the participants were asked to guess others' secret PIN.

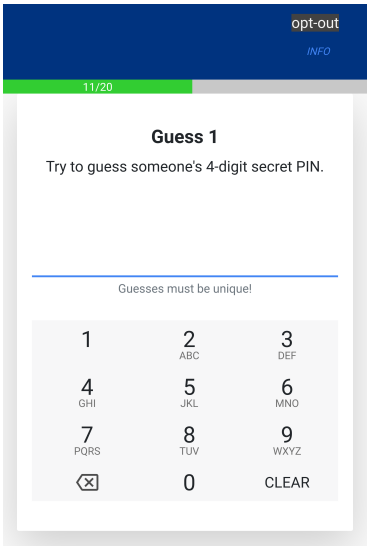


Figure 7: The page on which we asked participants to guess other participants' secret PIN.

E QUALITATIVE CODES

- **no (183)**
- **yes (134)**
- **pattern (127)**
  physical (2), word (2), sequential (1), odd-numbers (1)
- **simple (106)**
- **maybe (101)**
- **delegation (97)**
  entertainment (24), respond (11), find-information (7), shopping (4), location (3), take-photo (2)
- **partner (96)**
- **memorable (94)**
- **random (90)**
  guess (1)
- **date (89)**
- **guess (79)**
  personal-hint (51), shoulder-surf (12), smudges (1)
- **ask (63)**
- **shared (61)**
- **important-information (61)**
  financial (13), personal (13), sensitive (8), private (6), social-media (3), messages (2), email (2), confidential (2), apps (2), photo (1), health (1), photos (1), other-passwords (1), relationships (1), mature-content (1), encrypted (1), files (1), communication (1), browsing-history (1), contacts (1)
- **friend (58)**
- **family-member (58)**
- **personal-importance (56)**
  birthday (13), zip-code (3), date (2), partner (2), favorite-number (2), months (1), year (1), dat (1), name (1), acquaintance (1), lucky-number (1)
- **phone-locked (43)**
  pin (20), biometric (6), password (4), access (1), pattern (1)
- **find-information (41)**
  location (2)
- **physical-control (36)**
- **meaning (31)**
- **users-lazy (28)**
  unaware (1)
- **picked-common (28)**
- **nothing-to-hide (28)**
- **borrow-phone (26)**
  contact (12), find-information (5), entertainment (4)
- **dire-circumstances (25)**
- **reuse (24)**
- **hard-to-guess (23)**
  nobody-made-easy (3), needed-more-guesses (1), generation (1), not-enough-information (1), tricky (1)
- **picked-easy (23)**
- **privacy (22)**
- **mal-intent (21)**
- **picked-pattern (21)**
- **other-method (17)**
- **uncommon (17)**
- **picked-sequence (16)**
- **easy-to-guess (15)**
  simple (3), obvious (1)
- **unique (13)**
- **word (13)**
- **statistically-unlikely (12)**
- **picked-memorable (11)**
- **phone (10)**
- **picked-simple (10)**
- **shared-info (10)**
  financial (2), files (2), contacts (2)
- **other-pins-more-secure-than-irl (9)**
- **family-trusted (9)**
  partner (2)
- **undescribed (9)**
- **no-one (8)**
- **picked-easy-enter (8)**
- **trust-others (8)**
  acquaintances (2), familiar (1)
- **system (8)**
- **biometrics (8)**
- **curious (8)**
- **picked-random (8)**
- **laziness (8)**
- **unspecified (7)**
- **none (6)**
- **picked-repetition (6)**
- **guessed-by-luck (6)**
- **no-important-information (6)**
  financial (1)
- **malice (6)**
  financial (2), scam (1), manipulate-documents (1)
- **hard (6)**
  no-personal-info (1), no-feedback (1), others-mindset (1)
- **distress (5)**
- **thief (5)**
- **app-locked (5)**
- **picked-date (5)**
  year (3)
- **common (5)**
  numbers (1)
- **shared-passcode (4)**
  partner (1), family (1)
- **not-obvious (4)**
- **need-prior-knowledge (4)**
- **phone-insecure (4)**
  pin (3)
- **financial (4)**
- **number-users (4)**
  will-guess (1)
- **picked-other (3)**
  zip (1), no-strategy (1), diverse (1)
- **unconcern (3)**
- **security-questions (3)**
- **question-of-legality (3)**
- **not-pattern (3)**
- **zipcode (3)**
- **similar-thought-process (3)**
- **stranger (3)**
- **no-motive (2)**
- **resigned (2)**
- **police (2)**
- **luck (2)**
- **similar-reasoning (2)**
- **insecure (2)**
- **used-friends-pin (2)**
- **picked-insecure (2)**
- **brick-phone (2)**
- **lost-phone (1)**
- **smartphone-pin (1)**
- **not-complex (1)**
- **easily-change-password (1)**
- **not-difficult (1)**
- **multiple-attempts (1)**
- **boss (1)**
- **not-random (1)**
- **not-a-target (1)**
- **appearance (1)**
- **manufacturer-trust (1)**
- **no-knowledge (1)**
- **other-pins-more-simple-than-irl (1)**
- **cryptocurrency (1)**
- **no-pattern (1)**
- **convenient (1)**
- **search-warrant (1)**
- **phone-unlocked (1)**
- **number-participants (1)**
- **app-security (1)**
- **typical (1)**
- **need-consent (1)**