"The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 Digits

Collins W. Munyendo, *The George Washington University;* Philipp Markert, *Ruhr University Bochum;* Alexandra Nisenoff, *University of Chicago;* Miles Grant and Elena Korkes, *The George Washington University;* Blase Ur, *University of Chicago;* Adam J. Aviv, *The George Washington University*

https://www.usenix.org/conference/usenixsecurity22/presentation/munyendo

This paper is included in the Proceedings of the 31st USENIX Security Symposium.

August 10–12, 2022 • Boston, MA, USA

978-1-939133-31-1

Open access to the Proceedings of the 31st USENIX Security Symposium is sponsored by USENIX.

"The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 Digits

Collins W. Munyendo, Philipp Markert‡, Alexandra Nisenoff⋆,
Miles Grant, Elena Korkes, Blase Ur⋆, Adam J. Aviv
The George Washington University, ‡ Ruhr University Bochum, ⋆ University of Chicago

Abstract

With the goal of improving security, companies like Apple have moved from requiring 4-digit PINs to 6-digit PINs in contexts like smartphone unlocking. Users with a 4-digit PIN thus must "upgrade" to a 6-digit PIN for the same device or account. In an online user study ($n = 1010$), we explore the security of such upgrades. Participants used their own smartphone to first select a 4-digit PIN. They were then directed to select a 6-digit PIN with one of five randomly assigned justifications. In an online attack that guesses a small number of common PINs (10–30), we observe that 6-digit PINs are, at best, marginally more secure than 4-digit PINs. To understand the relationship between 4- and 6-digit PINs, we then model targeted attacks for PIN upgrades. We find that attackers who know a user's previous 4-digit PIN perform significantly better than those who do not at guessing their 6-digit PIN in only a few guesses using basic heuristics (e.g., appending digits to the 4-digit PIN). Participants who selected a 6-digit PIN when given a "device upgrade" justification selected 6-digit PINs that were the easiest to guess in a targeted attack, with the attacker successfully guessing over 25% of the PINs in just 10 attempts, and more than 30% in 30 attempts. Our results indicate that forcing users to upgrade to 6-digit PINs offers limited security improvements despite adding usability burdens. System designers should thus carefully consider this tradeoff before requiring upgrades.

1 Introduction

PINs are the most common form of smartphone unlock authentication; prior studies suggest that about 60% of users unlock their smartphone using a PIN [32]. As with other popular mobile authentication options, including Android unlock patterns [7, 35], LG Knock Codes [39], and passwords [34, 40], user-selected PINs for smartphone unlocking are chosen non-uniformly [14, 32, 51], leading to many common, insecure, and easily guessable PINs [32, 33, 51].

In response to the perceived insecurity of 4-digit PINs, which for years were the only PIN-length option for most smartphones, providers have begun to encourage or to require that users select a 6-digit PIN. For instance, with iOS 9, Apple transitioned from requiring 4-digit PINs to 6-digit PINs by default [6, 22]. Apple's own press release said that with passcodes "now [having] six digits instead of four . . . your passcode will be a lot tougher to crack" [6]. Similarly, an Ars Technica article about this change claimed that this "stronger passcode ups the ante" [22].

Prior work has compared the distribution of human-chosen 4-digit PINs to the distribution of human-chosen 6-digit PINs [32, 33, 51]. However, the impact of the upgrade process itself, in which a given user transitions from a 4-digit to a 6-digit PIN, has not been studied. In this paper, we thus explore the following research questions:

RQ1: How do users select a 6-digit PIN after having previously selected a 4-digit PIN?

RQ2: How does the upgrade process and the justification given impact the usability and security of 6-digit PINs?

RQ3: How predictable is a given user's 6-digit PIN if their previous 4-digit PIN is known to an attacker?

We conducted an online survey-based study ($n = 1010$) designed to model the important, real-world situations in which users upgrade their previously chosen 4-digit PIN to a 6-digit PIN. Using their own smartphone, participants were first directed to select a 4-digit PIN, specifically one they would use to protect their own smartphone. Participants were then prompted to change their 4-digit to a 6-digit PIN based on one of five treatments, each presenting a different scenario justifying the upgrade: (a) they upgraded their smartphone device and it now requires a 6-digit PIN; (b) their 4-digit PIN was leaked to someone they do not trust, necessitating a 6-digit PIN; (c) they are informed that their 4-digit PIN is guessed too easily, so they must now select a more secure 6-digit PIN; (d) a neutral reason, simply asking the participant to select a 6-digit PIN (as a control); (e) and, finally, using the same neutral scenario, but a blocklist was used such their 6-digit PIN could not contain their 4-digit PIN as a subsequence.

We analyzed the security of the 4- and 6-digit PINs using guessability metrics, including a perfect-knowledge and a simulated attacker, similar to prior work [13, 23, 32, 33]. In isolation, the 6-digit PINs participants selected offer limited security benefits over 4-digit PINs against an online attacker who can only make a few guesses (e.g., 10–30) before being locked out by the device, which is arguably the most common attack scenario for smartphone unlocking. This result is consistent with previously published analyses of the distribution of human-chosen 6-digit PINs [32, 33, 51]. Moreover, we observed differences across treatments regarding the 6-digit PINs selected. Notably, when prompted to select a 6-digit PIN because of a security issue, either due to the PIN being easily guessed or leaked, these 6-digit PINs were more difficult to guess compared to other treatments. However, device upgrading and, surprisingly, restricting 6-digit PINs to not contain the user's 4-digit PIN as a subsequence resulted in the least secure (most guessable) PINs. In many cases, these PINs were more easily guessed than the original 4-digit PIN.

Different from prior work, we also model a *targeted attacker* who leverages knowledge of the participant's (previous) 4-digit PIN in guessing their 6-digit PIN. Such an attacker models *how* users typically upgrade PINs, developing basic heuristics and patterns based on previously observed data (with the target user of course excluded). We find that a targeted attacker does substantially better than an untargeted attacker who guesses only common 6-digit PINs. Particularly troubling is that in the treatment most reminiscent of real-world scenarios (device upgrades requiring a 6-digit PIN, as with iOS 9), the targeted attacker can guess over 25% of the 6-digit PINs in 10 attempts, and over 30% in 30 attempts.

Similar to the limited security benefits of password expiration [18, 25, 43], where users must change their password after a fixed time, forcing PIN upgrades from 4 to 6 digits does not appear to significantly improve security. We found upgrades provide little or no benefit against targeted or untargeted online attacks. At the same time, 6-digit PINs negatively impact usability. System designers should thus carefully consider the limited security benefits of 6-digit PINs versus their negative impact on usability before requiring upgrades from 4-digit PINs. If upgrades are necessary, users must be encouraged to protect their seemingly obsolete 4-digit PINs as attackers can use them to guess their new 6-digit PINs.

2 Related Work

Prior research on mobile authentication has shown that PINs [14, 32, 33], Android unlock patterns [4, 5, 7, 35, 45], alpha-numeric passwords [34, 40] and LG Knock Codes [39] are selected non-uniformly by many users, making them susceptible to guessing attacks by both an untargeted [13, 32] and an informed attacker (e.g., a shoulder surfer) [8, 9, 10, 21, 48]. Many user-selected unlock patterns, for instance, begin in the top left corner of the grid and end in the bottom right corner [3, 7, 31, 35, 45, 49]. PINs are similarly predictable due to containing keypad sequences (e.g., `1234`) [51], repetitions, and birthdays [14, 16]. We observe similar patterns in the PINs we collect. While less common, alphanumeric passwords selected for mobile authentication tend to be weaker than those selected on computer keyboards [24, 34, 40, 47].

Several proposals have aimed to improve the security of PINs, including assigning users random PINs [41], changing how PINs are entered [12, 37, 46], augmenting PINs with additional information [15], and using blocklists that disallow common PINs [30, 32, 33]. Blocklists in particular have shown promise in improving the security of PINs [14, 30, 32], Android unlock patterns [35], and LG Knock Codes [39], especially if sufficiently large. Our study finds that blocklists that prohibit a user's 6-digit PIN from containing their 4-digit PIN as a subsequence help against a targeted attacker, yet unfortunately seem to encourage the selection of common 6-digit PINs easily guessed by an untargeted attacker.

The use of 6-digit PINs instead of 4-digit PINs has been recommended to users to improve their PIN security, for example by Apple since iOS 9 [6, 22]. However, prior studies have found that the security of 6-digit PINs selected by users against an online (untargeted) attack is not significantly different from the security of 4-digit PINs against an online (untargeted) attack [32, 33, 51]. In fact, 6-digit PINs are less secure and more easily guessable in some cases. The same phenomenon has been observed for unlock patterns, where a bigger grid size does not necessarily improve security [7]. Our study confirms these results for a throttled online attacker making up to 10 guesses. This further suggests that forcing users to upgrade from a 4-digit to a 6-digit PIN only marginally improves security while negatively impacting usability. Similar to password expiration policies, forcing a user to select a new authentication credential for arbitrary reasons can sometimes lead to decreased security, especially when effort was already made to select a secure password initially [18, 25].

Our work is most closely related to studies of 4- and 6-digit PINs by Markert et al. [32, 33] and Wang et al. [51]. However, whereas Markert et al.'s participants selected *either* a 4-digit PIN or a 6-digit PIN, our participants selected *both* a 4-digit and a subsequent 6-digit PIN, allowing us to model a targeted attacker that leverages knowledge of the participant's 4-digit PIN when guessing their 6-digit PIN. Compared to Wang et al., who constructed PINs artificially from leaked passwords, our study collects PINs from participants in a user study for ecological validity. Further, our study is the first, to the best of our knowledge, to specifically study how users upgrade from a 4- to a 6-digit PIN under various circumstances (e.g., when upgrading their device's operating system). While we similarly find that 6-digit PINs do not offer significant security benefits, we also find that a targeted attacker who knows a user's previously selected 4-digit PIN can easily guess their 6-digit PIN in many cases. We also find that security-oriented upgrade messages can make users select more secure PINs.

While we are, to our knowledge, the first to focus on targeted attacks on PIN upgrade scenarios, the more general idea of targeted attacker models is common in authentication research. Targeted attacks have successfully been used to guess alpha-numeric passwords [20, 36, 50]. More specifically, Das et al. [20] show that an attacker who knows one password of a user can leverage this knowledge to guess their passwords on other sites, while Wang et al. [52] show that a targeted attacker can benefit from a user's personal information (e.g., name, birthday) to guess their passwords. Shay et al. [43] also show that many users choose to modify their existing passwords when faced with a change in password policy. Our results confirm and expand on these results, demonstrating for the first time a targeted online attack for guessing 6-digit PINs based on previously selected 4-digit PINs.

3 Methodology

In this section, we describe the survey structure, followed by a detailed description of the five treatments used to prime participants in upgrading their 4- to a 6-digit PIN. We also discuss our recruitment, limitations, and ethical considerations.

3.1 Survey Structure

The first part of the survey consisted of each participant getting informed of the task and primed for smartphone unlock authentication. Afterward, the participants were directed to select a 4-digit PIN and then, due to different circumstances depending on the treatment, a 6-digit PIN. Additionally, participants were surveyed on their perceived security of each of the PINs, their strategies for selecting these PINs, and their preference between using the 4- or 6-digit PIN.

The survey was developed as an online web form, custom built to run on a smartphone, including the interface for entering PINs (see Figure 1 and 3). Participants were required to complete the survey on a smartphone, verified via their user-agent string. Below, we outline the procedures of the survey in more detail. The entire survey can be found in Appendix A.

1. *Informed Consent*: Participants were briefed about the purpose, duration, and risks associated with participating in the study. Participants had to consent to proceed.
2. *Practice:* To ensure familiarity with PINs and our interface, participants were asked to practice creating a single 4-digit PIN. These PINs were not used in our analysis.
3. *Instructions*: Participants were informed that they would now have to select a 4-digit PIN they would use to secure their smartphone. They were further informed that they would need to recall this PIN later in the survey, and therefore, it had to be both secure and memorable. Participants were additionally asked not to write down their PIN, and had to indicate they understood all these instructions before proceeding with the survey.
4. *Selection of 4-digit PIN*: Participants selected and confirmed a 4-digit PIN they would use on their smartphone.
5. *Questions about 4-digit PIN*: Participants were asked about their strategy to select their 4-digit PIN (**Q1**), whether they would use this PIN on their own smartphone (**Q2**) and their reason for or against doing so (**Q3**).
6. *Device Usage*: Before asking participants to select a 6-digit PIN, we asked them questions about their smartphone as a distractor task (**Q4** – **Q5b**).
7. *Recall of 4-digit PIN*: Participants were asked to recall their 4-digit PIN. If they could not do so in five attempts, they were moved on in the survey.
8. *Selection of 6-digit PIN*: After recalling their 4-digit PIN, participants were asked to select a 6-digit PIN. We phrased this differently depending on the assigned treatment (see Section 3.2). Figure 2 depicts the interface of this page including the way we highlighted the justification for upgrading the PIN.
9. *Questions about 6-digit PIN*: Participants were asked about their strategy to select their 6-digit PIN (**Q6**), and whether this PIN was related to their 4-digit PIN selected earlier (**Q7**). Participants were also asked whether they would use this 6-digit PIN on their smartphone (**Q8**), along with their reason for or against doing so (**Q9**).
10. *Further questions about 4-digit PIN*: To avoid priming the selection of the 6-digit PIN, we asked participants about the perceived usability and security of their 4-digit PINs only after they had selected both a 4- and 6-digit PIN (**Q10** – **Q13**). The 4-digit PIN was displayed to the participant for their reference. We also included the first of two attention check questions on this page (**Q14**).
11. *Recall of 6-digit PIN*: Participants were asked to recall their 6-digit PIN. If they could not do so in five attempts, they were moved on in the survey.
12. *Further questions about 6-digit PIN*: After displaying participants' 6-digit PINs for their reference, we asked about their perceived usability and security of these PINs on a Likert-scale (**Q15** – **Q18**). This page also included our second attention check (**Q19**).
13. *Comparison Questions*: Participants were asked whether they were more likely to use their 4- or 6-digit PIN, and their reasons for that. Further, participants were asked to compare the perceived usability and security of their 4-digit PIN against their 6-digit PIN (**Q20** – **Q24**).
14. *Demographics*: Participants were asked about their demographics including age, gender, dominant hand, level of education, and IT background. (**D1** – **D5**). In line with best practice [38], we asked these questions last to ensure they did not interfere with the study.
15. *Honesty*: Lastly, participants were asked if they had honestly participated in the study. Seven participants indicated dishonesty, and we subsequently discarded their responses from our final data analysis.

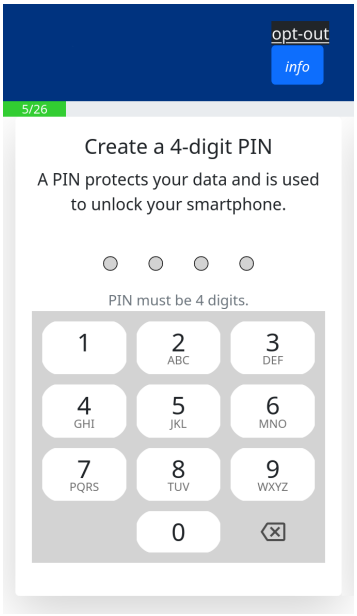


Figure 1: The design of the page on which we asked participants to create a 4-digit PIN.

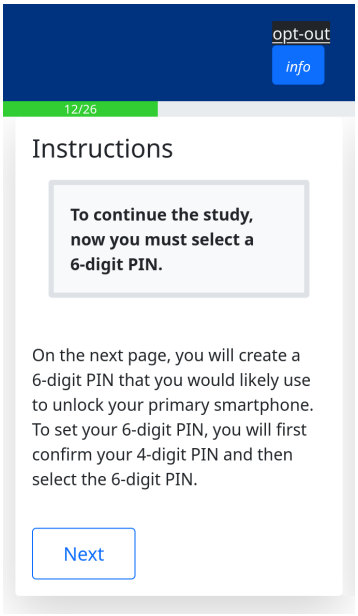


Figure 2: Instructions before 6-digit PIN creation. The text in the box varied by treatment (see Section 3.2).

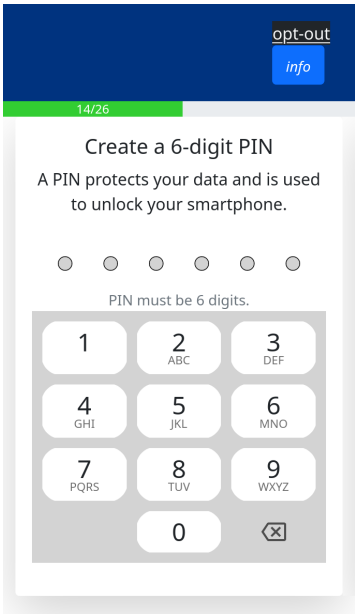


Figure 3: The design of the page on which we asked participants to create a 6-digit PIN.

3.2 Treatments

When upgrading to a 6-digit PIN from a 4-digit PIN, participants were randomly assigned to one of five treatments; neutral, breach, no-sub, security, and upgrade. Each of these treatments provided a different real-world scenario justifying the upgrade. The "upgrade" message that was displayed to participants in the neutral treatment is shown in Figure 2. The messages for all five treatments and some additional description is provided below:

- **Neutral** ($n = 201$): Participants in this treatment were asked to select a 6-digit PIN as follows: "To continue the study, now you must select a 6-digit PIN."
- **Breach** ($n = 203$): Participants in this treatment were asked to select a 6-digit PIN as follows: "Imagine someone learned your 4-digit PIN and to protect your smartphone, now you must select a 6-digit PIN."
- **No-sub** ($n = 205$): While participants in this treatment were asked to select a 6-digit PIN similarly to those in neutral, they were forbidden from using all 4 of the digits from their 4-digit PIN (in order) as a subsequence of their 6-digit PIN. For instance, if a participant's 4-digit PIN was `1234`, they could not select `001234`, `100234`, `120034`, `123004`, `123400`, `010234`, `012034`, `012304` etc. If the 4-digit PIN was a subsequence of the 6-digit PIN, we required the participant to select a new 6-digit PIN.
- **Security** ($n = 200$): Participants in this treatment were asked to select a 6-digit PIN as follows: "Research has shown that the 4-digit PIN you selected is insecure and can be easily guessed. To continue the study, now you must select a 6-digit PIN."
- **Upgrade** ($n = 201$): Participants in this treatment were asked to select a 6-digit PIN as follows: "Imagine you are upgrading your smartphone that requires PINs longer than 4-digits, and so now you must select a 6-digit PIN."

3.3 Recruitment and Demographics

Participants were recruited using Prolific, an online platform for matching participants with posted studies. After excluding 11 participants due to failing attention checks, dishonesty and inconsistencies, we had $n = 1010$ participants. They were compensated $2 for completing a nine-minute survey. The surveyed population comprised of younger (40% between 25–34), male-identifying (57% male, 41% female, and 2% other gender, or prefer not to say) participants with college education (30% some college or Associate's, 59% Bachelor's or above). Table 1 has the full demographic information.

3.4 Limitations

Our study has several limitations. First, as this was an online survey, it is not possible to determine if participants accurately followed all instructions. To mitigate this, we included two attention check questions (**Q14** and **Q19**) in the survey that helped us identify and remove four inconsistent responses.

Table 1: Participants' demographics.

	Male		Female		Other		Total	
	No.	%	No.	%	No.	%	No.	%
Age	579	57	411	41	20	2	1010	100
18-24	124	12	97	10	15	1	236	23
25-34	244	24	151	15	5	0	400	40
35-44	135	13	108	11	0	0	243	24
45-54	51	5	35	3	0	0	86	9
55-64	17	2	19	2	0	0	36	4
65-74	6	1	1	0	0	0	7	1
75+	1	0	0	0	0	0	1	0
Prefer not to say	1	0	0	0	0	0	1	0
Education	579	57	411	41	20	2	1010	100
Some High School	5	0	1	0	0	0	6	1
High School	59	6	33	3	3	0	95	9
Some College	104	10	89	9	9	1	202	20
Trade	11	1	14	1	0	0	25	2
Associate's	44	4	39	4	2	0	85	8
Bachelor's	219	22	148	15	5	0	372	37
Master's	111	11	69	7	1	0	181	18
Professional	14	1	10	1	0	0	24	2
Doctorate	11	1	8	1	0	0	19	2
Prefer not to say	1	0	0	0	0	0	1	0
Background	579	57	411	41	20	2	1010	100
Technical	190	19	46	5	4	0	240	24
Non-Technical	361	36	352	35	13	1	726	72
Prefer not to say	28	3	13	1	3	0	44	4

Additionally, we asked participants if they had honestly participated in the survey, promising to pay them even if they indicated dishonesty. Seven participants indicated dishonesty, and we did not consider their responses in our analysis.

Participants in our study may also suffer from fatigue due to having to select multiple PINs during the course of the survey. This may particularly affect the quality of 6-digit PINs as they were selected much later in the study. However, our 6-digit PINs closely match those collected by Markert et al. [32, 33] which were selected at the beginning of their study. Additionally, a majority of participants indicated they would use the 4- and 6-digit PINs they selected in this study on their smartphones, suggesting that the PIN selection observed in our study likely matches PIN selection in the real world. Nevertheless, future work leveraging longitudinal approaches is required to specifically explore how users upgrade their PINs over an extended duration of time.

Our instructions prohibiting participants from writing down their PINs may have skewed users to select PINs that are more memorable. However, users in fact carry their phones with them everywhere and may not always have their written-down PINs for reference. Further, our open-responses revealed that the strategies users employed in our study are consistent with strategies they use on their own smartphones, as well as strategies reported in other studies [14, 16]

The blocklist used in our no-sub treatment that barred users from using their 4-digit PIN as a subsequence in their 6-digit PIN differs significantly from traditional blocklists that prevent common choices, and which have been shown to improve security for PINs [32], unlock patterns [35] and Knock Codes [39]. Hence, our results should not be interpreted as an argument against blocklists, but rather ensure that blocklists are appropriately developed and sized to prevent user frustration that can ultimately limit their security benefits.

As is typical with Prolific and other crowdsourcing platforms, our surveyed population comprised mostly younger and well-educated participants. We do not claim our results to be representative of the general population; additional work is required to explore broader populations. Further, the recall rates captured in our study are short-term, as we were primarily interested in how users select 6-digit PINs, after selecting 4-digit PINs; exploring long-term recall rates is left for future work. Nonetheless, prior studies [7, 32, 39, 45] in mobile authentication indicate that short-term recall rates can provide reasonable measures of usability.

3.5 Ethical Considerations

This study was approved by our Institutional Review Board (IRB). Participants were fully informed about the purpose and risks associated with participating. We also considered the risk of the PINs selected as some participants indicated they use or would use these PINs on their smartphones. To mitigate any risks that would occur from a possible loss of confidentiality, we did not collect any personally identifying information from participants and analyzed the selected PINs separately from possible identifiers, such as their Prolific ID.

4 Features of Collected PINs

In this section, we describe features of common 4-digit and 6-digit PINs selected by participants, as well as strategies used to create them. Note, all participants selected their 4-digit PIN under the same conditions as the treatments only differed in the message displayed to create the 6-digit PIN (see Section 3.1). Lastly, we discuss similarities between 4- and 6-digit PINs that informed our targeted attacker's guessing strategies which are explained further in Section 5.3.

When discussing participant answers to qualitative, open-response questions, we developed a codebook to categorize these responses. This process involved a primary coder developing a codebook for a random subset of 30% (around 315) of the 1 010 responses, which offers a representative sample of the data. To verify the consistency of the codebook, a secondary coder used the codebook to code a subset of 20% (around 63) of the 315 responses, and then an inter-rater reliability score was calculated. If high agreement was reached ($\kappa > 0.7$), we considered the codebook verified, using the primary coder's responses. Otherwise the secondary coder met with the primary coder to update the codebook, and the process was repeated until agreement was reached.

Table 2: Common 4-digit PINs (frequency in brackets).

Treatment	4-digit PINs
Neutral	6969 (4), 1379 (3), 2580 (3), 0852 (2), 1981 (2), 2525 (2), 1245 (2), 2021 (2), 1997 (2)
Breach	2580 (4), 1995 (3), 2020 (3), 6969 (3), 0000 (2), 1470 (2), 1397 (2), 2543 (2), 7788 (2), 1234 (2)
No-sub	1234 (7), 2580 (5), 2468 (3), 1111 (3), 1478 (3), 1973 (2), 4444 (2), 3578 (2), 1010 (2), 0921 (2)
Security	1212 (4), 0000 (4), 1337 (3), 1397 (2), 1125 (2), 2486 (2), 1970 (2), 1379 (2)
Upgrade	1256 (3), 1313 (3), 6969 (3), 1337 (3), 1234 (3), 1776 (2), 2580 (2), 5858 (2), 1258 (2), 5683 (2), 2222 (2), 9876 (2), 0007 (2)

Common 4-digit PIN Features The resulting codebook for **Q1**, which can be found in Appendix B, revealed that most participants use different techniques to make their 4-digit PINs memorable. Similar to prior work [14, 16, 51], participants mostly used important dates, particularly birthdays, when selecting 4-digit PINs. For instance, P68 said "I decided to use my birthday because it is something that I will never forget." The use of personal information such as subsets of phone numbers or addresses is also common, suggesting that an attacker who has access to such information can easily guess these PINs. For example, P387 used digits from a phone number: "Last 4 digits of phone numbers I know and use often." Other common techniques include selecting PINs that are easy to enter, or based on repetitions and keypad patterns. Perhaps unsurprisingly, participants did not mention security as being a driving factor in their choice of PIN, with only a few participants indicating that they selected PINs specifically such that they were difficult to guess. This confirms prior work where most users prefer convenience over security when selecting credentials [26, 29, 33].

Participants' 4-digit PIN selection strategies are further confirmed by analyzing the actual PINs they selected (see Table 2). In the neutral treatment, the most common PIN is `6969` (4) followed by `1379` (3) and `2580` (3), which all follow keypad patterns. While `2580` (4) is the most common PIN in the breach treatment, we find that years, such as `1995` (3) and `2020` (3), are also common, as well as `6969` (3). The most common PIN in no-sub is `1234` (7), an increasing sequence of the first four digits on the keypad. Other PINs that form patterns on the keypad for example `2580` (5), `2468` (3), and `1478` (3) are also common, as well as repetitions such as `1111` (3). In the security treatment, repetitions such as `1212` (4), `0000` (4), and `1337` (3) are very common, similar to the upgrade treatment, where `1313` (3), and `6969` (3) are the most popular. Sequences such as `1234` (3) are also common as well as PINs that form patterns on the keypad such as `1256` (3). Generally, we find that the most common 4-digit PINs in our study are similar to those observed in prior literature [14, 51].

Table 3: Common 6-digit PINs (frequency in brackets).

Treatment	6-digit PINs
Neutral	123456 (4), 121212 (3), 062488 (2), 159357 (2), 654321 (2), 456789 (2), 085213 (2)
Breach	139755 (2), 696969 (2), 778899 (2)
No-sub	123456 (8), 134679 (3), 147896 (3), 135790 (2), 222222 (2), 888888 (2)
Security	123789 (2), 666666 (2), 867530 (2)
Upgrade	123456 (7), 696969 (3), 131313 (2)

Common 6-digit PIN Features In **Q6**, we asked participants about their selection strategies for a 6-digit PIN, and performed a qualitative analysis of the responses (codebook in Appendix B). The coding revealed that most participants create memorable 6-digit PINs, similar to 4-digit PINs. Again participants appear to mostly use dates, more specifically different variations of their birthdays. P7, e.g., mentions using their birthday even though it makes the PIN inherently insecure: "It's my birthday; I know, that's basically zero security." P7 further elaborated that it makes the PIN memorable: "It's my birthday, [therefore it's] easy to remember."

The use of personal information, such as phone numbers, addresses, or favorite numbers is another common technique, with P247 saying "I am using [the] last 6 digit[s] of my phone number." Keypad patterns are also common, as well as reuse of previously created 6-digit PINs. Unless they were in the no-sub treatment, many participants also indicate modifying their 4-digit PIN. We will describe in Section 5.3 how we leveraged this information to build a targeted attacker for 6-digit PINs.

Participants' 6-digit PIN strategies are once again confirmed when we analyze the PINs they selected (see Table 3), with sequences and repetitions being widely used. In the neutral treatment, sequences such as `123456` (4) and repetitions like `121212` (3) comprise the most common PINs, as is the case in breach where `696969` (2), and `778899` (2) are the most common. `123456` (8) is overwhelmingly popular in the no-sub treatment, perhaps as a result of users getting frustrated when subsequences of their 4-digit PIN are blocked. Other common PINs in this treatment such as `134679` (3), `147896` (3), and `135790` (2) follow a pattern on the keypad, with repetitions such as `222222` (2) and `888888` (2) being common as well. In security, patterns, e.g., `123789` (2) and repetitions such as `666666` (2) are common while in upgrade, the sequential PIN, `123456` (7) is by far the most popular. Still, repetitions such as `696969` (3) and `131313` (2) are also common.

Generally, the 6-digit PINs selected in the security and breach treatments are slightly more unique, with the most common 6-digit PIN only selected twice. In the the other treatments, the most common 6-digit PIN appears at least four times. While this possibly indicates that security-oriented upgrade messages are beneficial for security, 6-digit PINs selected were not meaningfully different from 4-digit PINs overall, suggesting limited security benefits of 6-digit PINs over 4-digit PINs, confirming prior work [32, 33, 51].

Table 4: Frequency of the most common PIN modifications; no-sub is excluded as these modifications were disallowed.

Modification	Treatment				
	Neutral $n = 201$	Breach $n = 203$	Security $n = 200$	Upgrade $n = 201$	Total $n = 805$
Appends	71	80	68	93	312
Prepends	14	14	14	14	56
Insertions*	15	4	7	18	44
None of the above	107	110	114	85	416

*: excluding appends and prepends.

Similarities between 4- and 6-digit PINs In comparing the open responses from **Q1** and **Q6**, as well as the PINs selected, we find that most participants use similar strategies for creating both 4- and 6-digit PINs. This includes using subsets of personal information such as phone numbers and addresses, repetitions, and important dates. Most participants describe doing so to make the PINs easier to remember. When allowed, many participants chose to incorporate their 4-digit PIN into their 6-digit PIN, often by adding two digits to their chosen 4-digit PIN. For example, P204 said "I used the same first four digits as the last time, but added a couple more at the end" while P227 added that it is "the same PIN, just longer."

Table 4 describes how often participants chose to append, prepend, or insert digits to their 4-digit PIN to create their 6-digit PIN. In cases where a modification could be either an append or prepend, as in `1111` → `111111`, we counted it for both categories. The common modifications observed form the bases for the targeted attacker's guessing strategies. While restricting the use of the 4-digit PIN in creating the 6-digit PIN is a tempting technique to restrict such behavior, we find that this may actually decrease the quality of the 6-digit PINs, leading to more guessable and insecure PINs. We will discuss this in more detail in the following Section 5.

5 Security Analysis

In this section, we discuss the security analysis of the 4- and 6-digit PINs selected by participants in the study. We begin by describing the datasets that are used to train the three attacker models considered: two untargeted attackers and one targeted attacker. For the untargeted attacker model, we first consider the perfect knowledge scenario where the attacker has complete knowledge of the distribution of the PINs being guessed, and then we consider a simulated attacker that guesses PINs by using a known distribution of PINs, such as a leaked dataset. Finally, we present the results of a targeted, simulated attacker that has knowledge of the 4-digit PIN the target selected in attempting to guess their 6-digit PIN.

In each of the attacker models, we are primarily concerned with the security of PINs against a throttled, online attack where the attacker only has a limited number of attempts to guess the PIN and access the device. An offline, unlimited attacker, typically considered for password guessability, is not meaningful for PINs as the small credential space (10 000 4-digit PINs and 1 000 000 6-digit PINs) would be trivially cracked. Hence, Android and iOS limit the number of incorrect attempts to unlock the phone before implementing extensive delays, on the order of minutes or hours. If sufficient incorrect guesses are made, the device could even be wiped and deactivated. On iOS, this occurs after 10 incorrect guesses, and on Android, an attacker can attempt 30 guesses in roughly one hour before experiencing significant delays between attempts. Therefore, we consider an attack successful if it can be completed within 10 to 30 guessing attempts.

5.1 Datasets

For the untargeted and targeted simulated attackers, the guessing model requires knowledge of known distribution of PINs. To train the 4-digit PIN models, we used a dataset collected by Daniel Amitay [2], so called Amitay dataset, released by Amitay as part of an iOS app that mimicked a lockscreen. The Amitay dataset contains 204 432 4-digit PINs [2] from users. Prior work suggests, that for a simulated attacker, the Amitay dataset is perhaps the most realistic and offers a significant advantage over PINs derived from leaked password datasets [32, 33]. We confirm this in our study (see Figure 4).

When guessing 6-digit PINs, there is no analogous dataset to use, and as such we use 6-digit PINs that were extracted from numeric sequences in the RockYou passwords leak [19]. A 6-digit PIN was determined when an exact sequence of 6-digits was found in a password, such as `123456` from the password `love123456done`, but not the PIN `123456` nor `234567` from the password `love1234567done`. The same approach has been used by Bonneau et al. [14], Wang et al. [51], and Markert et al. [32, 33] to study 6-digit PINs in prior research. We refer to this dataset as the RockYou dataset.

5.2 Untargeted Attacker

We first use an untargeted attacker to analyze 4- and 6-digit PINs. We describe this attacker model as "untargeted" as it treats all victims equally with respect to the guessing strategy. We consider two variations of this attacker: first, a *perfect knowledge attacker* that knows the exact distribution of the PINs to guess, providing an upper bound on the guessing performance for an untargeted attacker, and second, a simulated attacker that uses a training dataset of PINs to guess an unknown set of PINs. The training datasets comprise of 4-digit PINs from the Amitay dataset and 6-digit PINs from the RockYou dataset, as described earlier. The guessing order is determined by sorting the training dataset of PINs in frequency order, guessing the most frequent PIN first. When two PINs have the same frequency, ties are broken using a Markov model, as described and recommended in prior work [17].

Table 5: Guessing performance of a perfect knowledge attacker.

	Throttled Attack (%)						Unthrottled Attack (Bits)							
	λ_3		λ_{10}		λ_{30}		H_∞		$\widetilde{G}_{0.1}$		$\widetilde{G}_{0.3}$		$\widetilde{G}_{0.5}$	
Treatment	4-digit	6-digit	4-digit	6-digit	4-digit	6-digit	4-digit	6-digit	4-digit	6-digit	4-digit	6-digit	4-digit	6-digit
Neutral	4.5%	4.5%	11.0%	10.0%	21.0%	20.0%	5.64	5.64	6.49	6.71	7.55	7.61	7.87	7.90
Breach	5.0%	3.0%	12.5%	6.5%	22.5%	16.5%	6.06	6.64	6.32	7.48	7.46	7.80	7.82	8.01
No-sub	7.0%	7.0%	14.5%	12.0%	24.5%	22.0%	4.84	4.64	5.90	5.97	7.32	7.49	7.75	7.84
Security	5.5%	3.0%	11.5%	6.5%	21.5%	16.5%	5.64	6.64	6.32	7.48	7.52	7.80	7.85	8.01
Upgrade	4.5%	6.0%	12.5%	9.5%	24.0%	19.5%	6.06	4.84	6.32	6.85	7.36	7.64	7.77	7.92

Perfect Knowledge Attacker Table 5 presents the perfect knowledge attacker results, for both 4- and 6-digit PINs. Note, all participants selected their 4-digit PIN under the same conditions as the treatments only differed in the message displayed to upgrade to 6 digits (see Section 3.1). To fairly compare the treatments with different number of examples, we randomly down-sampled all treatments to the size of the smallest treatment, i.e., security. We use the β-*success-rate* and α-*guesswork* metrics defined by Bonneau [13] to assess the performance of our perfect knowledge attacker in both a throttled and an unthrottled scenario.

The β-success-rate refers to the percentage of PINs guessed after β guesses. Therefore, it describes an attacker who is constrained in the number of guesses they can make. Presented as λ_β in Table 5, we find that 6-digit PINs do not meaningfully differ from 4-digit PINs in terms of security, confirming prior research [32, 33, 51]. Using the neutral treatment for a fair comparison, the attacker's success rate slightly reduces from 21.0% (4-digit) to 20.0% (6-digit) of PINs guessed after 30 guesses. However, the scenarios in the treatment appear to effect the security of 6-digit PINs, with those selected in the breach and security treatments appearing harder to guess compared to the neutral treatment. For example, when making up to 30 guesses, a perfect knowledge attacker's success rate decreases from 22.5% (4-digit) down to 16.5% (6-digit) in the breach treatment while in the security treatment, the attacker's performance reduces from 21.5% (4-digit) to 16.5% (6-digit) of PINs successfully guessed. This suggests that security-oriented upgrade messages can improve the security of user-selected PINs during upgrades.

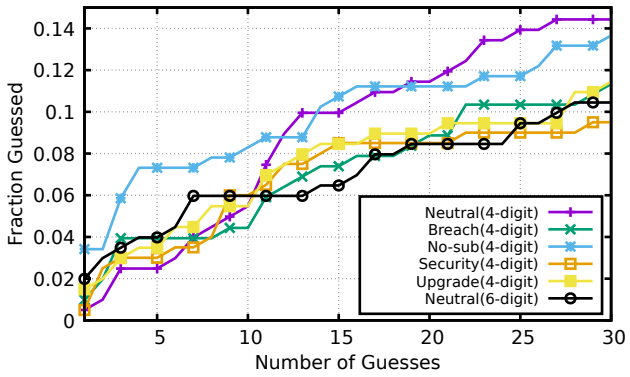
Interestingly, for a perfect knowledge attacker, we do not find meaningful security benefits in blocking participants' 4-digit PINs appearing as a subsequence in their 6-digit PINs. The attacker guesses a similar fraction (7.0%) of both 4- and 6-digit PINs after 3 guesses. When making up to 10 guesses, the attacker's performance slightly reduces from 14.5% (4-digit) to 12.0% (6-digit) of PINs successfully guessed, and from 24.5% (4-digit) to 22.0% (6-digit) when making up to 30 guesses. This attacker also appears to guess more 6-digit PINs in this treatment compared to all other treatments. However, it must be noted that 4-digit PINs selected in this treatment were also more easily guessable compared to other treatments. Nonetheless, blocking participants' 4-digit PIN subsequences in the 6-digit PIN had limited security improvement, sometimes leading to more guessable 6-digit PINs.

The α-guesswork models an attacker unconstrained in the number of guesses they can make. It measures the amount of "work" in bits of entropy, required to guess an α fraction of the PINs in the target dataset (i.e., how difficult it is to guess a certain fraction of the PINs). A higher entropy means the attacker requires more guess work and therefore, the PINs are more secure. Our unthrottled perfect knowledge attacker results are indicated by $\widetilde{G}_\alpha$ in Table 5.

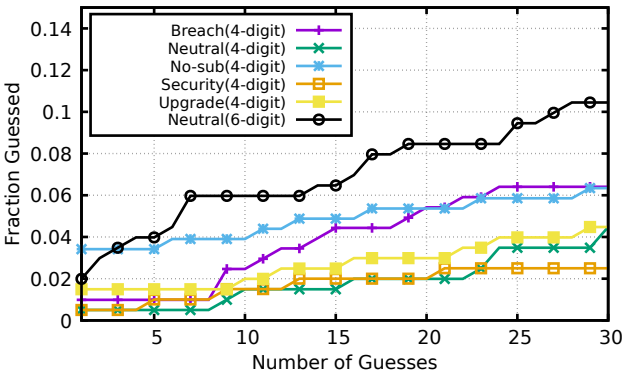
Similar to the throttled attacker results, we find that 6-digit PINs selected are not meaningfully more secure than the 4-digit PINs. In the neutral treatment, the attacker needs 7.90 bits to guess half of the 6-digit PINs, a small increase of 0.03 bits in comparison to guessing a similar fraction of 4-digit PINs. However, we once again find that security-oriented upgrade messages can be helpful, with this attacker requiring 0.16 more bits in security, and 0.19 more bits in breach to guess half of the 6-digit PINs compared to 4-digit PINs.

At the same time, it appears that an unthrottled attacker often requires less "work" to guess 6-digit PINs in the no-sub treatment compared to all other treatments. Particularly interesting, this attacker requires less "work" (0.20 bits) to guess the most common 6-digit PIN (4.64) compared to the most common 4-digit PIN (4.84) in this treatment. This suggests that blocking subsequences of users' 4-digit PINs in their 6-digit PINs does not necessarily increase security of the selected 6-digit PINs for an unthrottled attacker; in fact, it may make the 6-digit PINs less secure, particularly if the 4-digit PINs were already reasonably secure. These results are further confirmed by the simulated attacker below.

Simulated Attacker Figure 4 shows the simulated attacker results for 4-digit PINs, as well as 6-digit PINs in the neutral treatment ($\circ$). Note that all participants selected 4-digit PINs under the same conditions, and the differentiation by treatment is only to provide a point of comparison to the upgraded 6-digit PIN. Figure 4a shows the performance of this attacker when using the Amitay dataset to guess 4-digit PINs and RockYou to guess 6-digit PINs while Figure 4b shows the attacker performance when using RockYou to guess both 4- and 6-digit PINs. Our results confirm prior work [32, 33] that has shown that the Amitay dataset performs significantly bet-



(a) Performance using Amitay for 4- and RockYou for 6-digit PINs.



(b) Performance using RockYou for both 4- and 6-digit PINs.

Figure 4: Performance of an untargeted simulated attacker when guessing 4- and 6-digit PINs.

ter at guessing 4-digit PINs. Hence, we base our discussions on Figure 4a as we assume an attacker would use the best training material. The untargeted simulated attacker performs similarly across breach (×), upgrade (■), and security (□), but slightly better in no-sub (∗) and neutral (+) treatments.

These results further confirm that 6-digit PINs are not meaningfully more secure than 4-digit PINs, in line with prior work [32, 33]. In fact, they are sometimes less secure. When making up to 10 guesses, the simulated attacker can guess 6.0% of 6-digit PINs in the neutral treatment (see Figure 4a), more than the 5.5% of 4-digit PINs guessed in the same treatment after a similar number of guesses. When making up to 30 guesses, the attacker guesses 10.4% of 6-digit PINs and 14.4% of 4-digit PINs. In other treatments, the performance of 4-digit PINs is similar to the neutral 6-digit PIN treatment—recall that the selection of 4-digit PIN is unaffected by the treatment—where in some cases, the same fraction of 4-digit PINs are guessed as 6-digit PINs, or even fewer. Note that even when RockYou is used to guess both 4- and 6-digit PINs (see Figure 4b), 6-digit PINs still remain insecure.

Similar to the perfect knowledge attacker, the treatments that involve a security priming, either breach or security, lead to PINs that are harder to guess, compared to the neutral, device upgrade, and no-sub treatments (see Figure 6a). After 30 guesses, the simulated attacker guesses 10.4% and 9.0% of 6-digit PINs in the neutral and upgrade treatments respectively, but only 4.5% and 4.4% of PINs in the security and breach treatments respectively. This suggests that security-oriented upgrade messages can encourage selection of secure PINs.

Strikingly, the no-sub condition leads to the most guessable 6-digit PINs in the untargeted simulated attacker model when making up to 30 guesses. Likely, as participants could not use subsequences of 4-digit PINs they were familiar with due to the blocking, they fell back to less secure 6-digit PIN choices that were more common in the training dataset. This runs counter to our intuition about this treatment and indicates that some interventions, even when well-intentioned, can lead to unintended side effects.

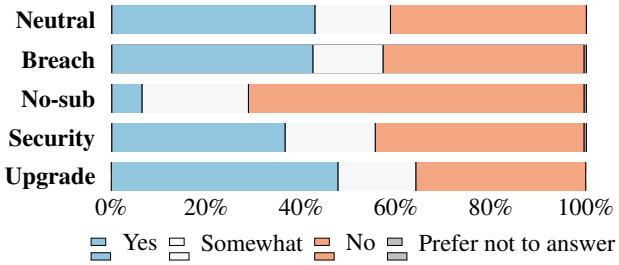


Figure 5: Participants' responses to question **Q7**: "Is your 6-digit PIN related to your 4-digit PIN?"

We performed a χ^2 test to compare guessing 4-digit PINs using Amitay (see Figure 4a) vs. 6-digit PINs using RockYou (see 6a) in the untargeted throttled attacker setting for 3, 10, and 30 guesses. We find no significant differences across all treatments except in one case: when the attacker is making 30 guesses in the breach treatment, 4-digit PINs were significantly less secure than 6-digit PINs ($\chi = 36.73$, $p = 0.02$). When RockYou is used to guess both 4- and 6-digit PINs, there are no differences except in the neutral treatment. In this case, significantly less 4-digit PINs are guessed after 10 ($\chi = 30.51$, $p = 0.03$) and 30 guesses ($\chi = 40.05$, $p = 0.04$). Still, this suggests that most 6-digit PINs are not significantly different from 4-digit PINs in terms of their resistance against untargeted throttled attacks.

5.3 Targeted Attacker

Many participants indicated that their 6-digit PIN was related to their 4-digit PIN (see Figure 5), except in the no-sub treatment. Motivated by this relationship, we developed a targeted attacker that assumes knowledge of the victim's 4-digit PIN prior to switching to a 6-digit PIN. We first describe the targeted guessing strategies and the guessing algorithm, Afterwards, we discuss the performance of this attacker.

Algorithm 1 Targeted guessing for 6-digit PINs.

```
GuessingOrder ← [ ]
GuessStrategies ← Targeted strategies & collected 6-digit PINs with Frequency ≥ 2
UserPINs ← List of (4-digit, 6-digit) PINs for each user
while NOT UserPINs == [ ] do
    BestStrategyCount ← 0
    BestStrategy ← None
    for S in GuessStrategies do
        CorrectGuessesS ← Number of correct guesses S could make in UserPINs
        if CorrectGuessesS > BestStrategyCount then
            BestStrategyCount ← CorrectGuessesS
            BestStrategy ← S
        end if
    end for
    if BestStrategyCount == 0 then
        break
    else
        GuessingOrder.append(BestStrategy)
        UserPINs ← UserPINs NOT guessed by BestStrategy
    end if
end while
RockYou ← List of 6-digit PINs from RockYou in descending frequency order
for PIN in RockYou do
    if NOT PIN in GuessingOrder then
        GuessingOrder.append(PIN)
    end if
end for
return GuessingOrder
```

Targeted Guessing Strategies As a targeted attacker model is novel in this space, we develop a set of guessing strategies based on analyzing how participants upgrade from 4- to 6-digit PINs. Importantly, for each strategy, we remove the example of the victim's 4-digit and 6-digit PIN pairs to avoid over-fitting. The attacker, however, is assumed to have broad knowledge of how users upgrade their PINs and the distribution of the 6-digit PINs based on the collected sample data, but not the 6-digit PIN of the victim being targeted.

As shown in Table 4, appending digits to the 4-digit PIN is the most common strategy for upgrading to a 6-digit PIN, followed by prepends and insertions. We additionally observe cases where all the 4 digits from the 4-digit PIN appear in the 6-digit PIN, but not in order. As such, a targeted attacker should leverage these patterns in generating 6-digit guesses from 4-digit PINs. We also observed that only certain digit sequences, such as `00`, were commonly appended or prepended, so the attacker does not need to exhaust the space of possible additions to the 4-digit PIN, but rather just consider the most common cases. More specifically, we consider the following strategies when generating our initial guess order:

1. **Targeted Appends**: The attacker considers the structure of the 4-digit PIN and assumes the target appended either: (a) the first two digits, for example, `1234` → `123412` (occurring 45×); (b) the last two digits repeated, for example, `1234` → `123434` (40×); (c) the last digit twice, for example, `1234` → `123444` (29×); and, (d) the inner-two digits, for example, `1234` → `123423` (15×).

2. **Common Appends**: The target appends a two-digit sequence to their 4-digit PIN. The most popular appends observed in the data are `00` (occurring 24×), `69` (21×), `11` (13×), `12` (11×), `99` (9×), `36` (9×), `88` (8×), `55` (8×), and `13` (8×). Therefore, the attacker appends these sequences, for example, `1234` → `123400`, `123469`, etc.

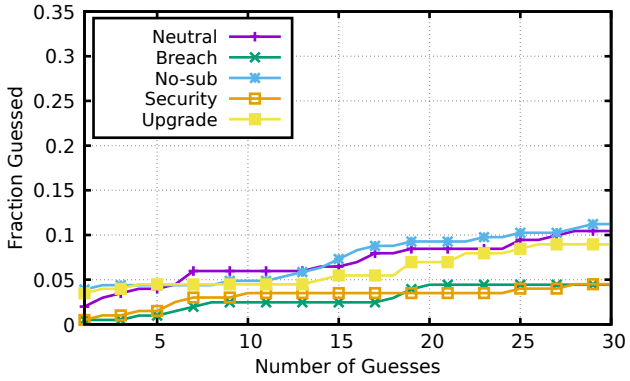
3. **Common Prepends**: The target prepends a two-digit sequence to their 4-digit PIN. The only common prepending sequence observed was `00`, specifically `1234` → `001234` (occurring 8×).

4. **Distribution of 6-digit PINs**: The attacker knows the distribution of 6-digit PINs selected by other participants. Some of the most common 6-digit PINs observed in our data include `123456` (occurring 21×), `696969` (7×), `121212` (5×), `654321` (5×) and `159357` (5×).

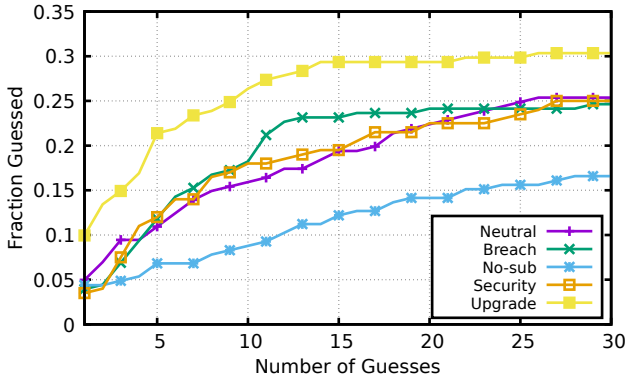
Table 6: First 30 guesses made by the targeted attacker. If a strategy generated a duplicate PIN, that PIN was skipped.

Strategy	Guessing Strategy	Guesses
Append first two digits	Targeted Append	45
123456	Collected PINs	21
Append the last digit twice	Targeted Append	20
Append 69	Common Append	16
Append 00	Common Append	15
Append the last two digits	Targeted Append	13
Append 11	Common Append	9
Append 12	Common Append	8
Append 36	Common Append	8
Append 99	Common Append	8
Append 55	Common Append	7
Append 88	Common Append	6
Append the inner two digits	Targeted Append	5
654321	Collected PINs	5
159357	Collected PINs	5
Prepend 00	Common Prepend	4
123789	Collected PINs	4
134679	Collected PINs	4
Append 13	Common Append	3
666666	Collected PINs	3
121212	Collected PINs	3
987654	Collected PINs	3
888888	Collected PINs	3
456789	Collected PINs	3
147258	Collected PINs	3
147369	Collected PINs	3
147896	Collected PINs	3
867530	Collected PINs	3
222222	Collected PINs	2
696969	Collected PINs	2

While other transformational patterns from 4-digit PINs to 6-digit PINs exist and were observed in the data, such as using keypad patterns, relying solely on these can lead to extraneous guesses that are not easily ordered in terms of their likelihood. Instead, we include the relatively conservative set of strategies discussed, and it is important to note that these techniques may represent a lower bound on the ability of a targeted attacker. There may be strategies that were not considered here that would be beneficial. However, even these conservative set of strategies greatly benefit a targeted attacker with just a limited number of guessing attempts.



(a) Performance using only the RockYou dataset.



(b) Performance using RockYou and targeted guessing strategies.

Figure 6: Performance of an untargeted versus a targeted simulated attacker when guessing 6-digit PINs.

Targeted Guessing Algorithm The guessing order should be optimized to most advantage the attacker. Therefore, we determined the most optimal order for our initial guesses using the targeted strategies described earlier. This generated a set of 6-digit PINs to guess first, and if the PIN of the victim was not guessed within these set of guesses, we proceeded to guess using 6-digit PINs obtained from the RockYou dataset. Note that we excluded the 4- and 6-digit PIN pairs of the victim from our targeted strategies to avoid over-fitting.

For each of our targeted strategies, we determined the number of correct guesses that the strategy would make, focusing on guesses that had not been already made by any of the other strategies. Thereafter, we selected the strategy that made the next most correct guesses, breaking ties based on the PINs frequency rank in the RockYou dataset. We iteratively repeated this process until all the 6-digit PINs had been guessed. If the PIN could not be guessed using our targeted strategies, we used 6-digit PINs from the RockYou dataset to make further guesses. These PINs were ordered in a descending order of frequency. Algorithm 1 provides high level pseudocode for our simulated targeted attacker.

Through this technique, we found that appending the first two digits of a user's 4-digit PIN was the most effective guessing strategy for their 6-digit PIN, as it could correctly guess 45 6-digit PINS (4.5% of the total number of the PINs and more than twice what would have been guessed by an untargeted attacker with a single guess). Guessing `123456`, a common 6-digit PIN, yielded the next highest number of correct guesses from the remaining 6-digit PINs, followed by appending the last digit of the 4-digit PIN repeated. This was followed by appending 69, 00, the last two digits of the 4-digit PIN, 11, 12, 36, and 99. Table 6 contains the initial 30 guesses made by the targeted attacker.

For each treatment, there are some PINs that are guessed relatively faster (see Table 6), greatly benefiting the attacker. At the same time, some PINs are guessed later in the guessing order that would have been guessed sooner, disadvantaging the attacker. However, this has limited impact in the online attack setting of mobile devices, where the attacker only has a few (10–30) attempts to guess the PIN. The benefits from correctly guessing more PINs sooner greatly outweigh guessing more PINs later, particularly for PINs that would have been guessed outside the throttled cutoff (over 30 guesses).

Using this analysis, the final targeted guessing algorithm generates an initial guessing order of 6-digit PINs using the targeted strategies we have described. The remaining guesses occur using 6-digit PINs obtained from the RockYou dataset, guessing in decreasing frequency order similar to the untargeted attacker model. In the no-sub treatment, the targeted attacker guesses using the RockYou dataset but skips 6-digit PINs that could not have been selected due to the treatment. It is again important to note that for each target, their 6-digit PIN is excluded from the training data used to guess possible 6-digit PINs that the target selected to avoid overfitting.

Targeted Guessing Performance Figure 6b shows the success rate of the targeted attacker in guessing a fraction of the 6-digit PINs after a certain number of attempts, and we observe large differences between treatments. The worst performing treatment is device upgrade, where after only 10 guesses, a targeted attacker is able to guess 26.4% of 6-digit PINs, compared to 4.5% guessed by an untargeted attacker. In contrast, this attacker guesses 18.2% of 6-digit PINs in the breach treatment, 18.0% in security, 15.9% in neutral and 8.8% in no-sub after a similar number of guesses. This is similar when making up to 30 guesses, with this attacker guessing 30.3% in upgrade, 24.6% in breach, 25.4% in neutral, 25.0% in security and 16.6% in the no-sub treatment. The attacker's performance slightly improves in the no-sub treatment since the attacker can skip 6-digit PINs that could not be selected by participants due to being blocked as part of the treatment.

We performed a χ^2 test to compare the guessing performance between a targeted and an untargeted attacker for 6-digit PINs in a throttled setting (3, 10 and 30 guesses). We find that a targeted attacker performs significantly better across

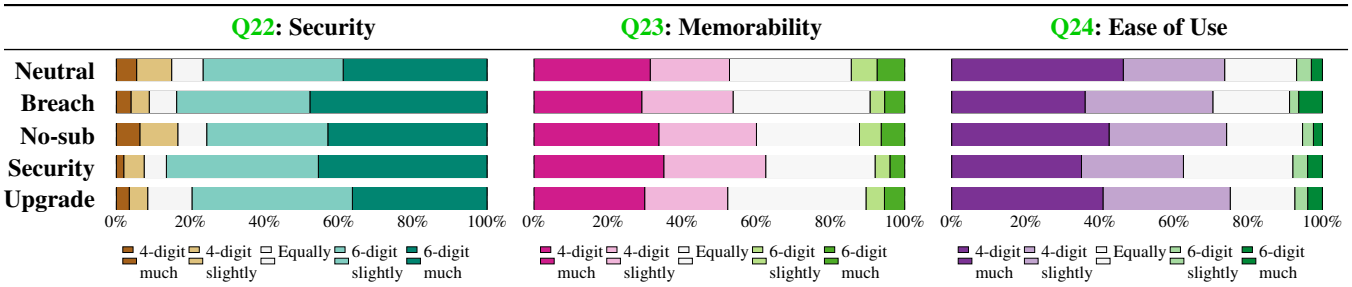


Figure 7: Participants' perception of whether their 4- or 6-digit PIN is more secure, easier to remember, and easier to use.

all treatments except the no-sub treatment. This is not surprising as we prevented participants from selecting 6-digit PINs with subsequences of their 4-digit PINs in this treatment, and the slight improvement (see Figure 6) was as a result of the targeted attacker having knowledge of the distribution of 6-digit PINs. These results are consistent when the targeted attacker is compared to an untargeted attacker that knows the distribution of 6-digit PINs selected by other participants.

These results suggest that encouraging upgrades, even when threats are clearly communicated, can result in 6-digit PINs that are easily guessable in the targeted attack setting (see Figure 6b). While blocking subsequences of the 4-digit PIN offers protection from targeted attacks, it is also the worst performing treatment in the untargeted attack model (see Section 5.2), and thus may not be a good solution. Instead, these results suggest that the security benefits of upgrading PINs from 4- to 6-digits are minimal, similar to the limited security benefit of policies that require users to change their passwords often. Users should instead be encouraged to select a secure PIN once, either 4- or 6-digit, rather than require upgrades. Where device upgrades are necessary, it is important to encourage users to protect their seemingly obsolete 4-digit PIN as it can leak information about their 6-digit PIN.

6 User Perception and Preference

In this section, we discuss user preferences and perceptions of their PINs with respect to security, memorability, and ease of use. The full set of codes is available in Appendix B, and was developed using the same process outlined in Section 4.

User Perception We asked a set of questions to learn how users perceive the security, memorability, and ease of use of their PINs. We did this separately for participants' 4-digit (**Q10** – **Q13**) and 6-digit PINs (**Q15** – **Q18**) as well as in comparison to each other (**Q22** – **Q24**).

When asked about the security of their 4-digit PINs, most participants feel their choice is "secure" or "somewhat secure", ranging from 54% in the no-sub treatment to 61% in breach. Interestingly, participants in breach still perceive their 4-digit PIN as secure, despite being informed that someone else has learned this PIN. When asked to explain this in **Q11**, qualitative coding revealed that only a few participants consider that someone else has learned about their PIN. Instead, most participants believe their PIN is unlikely to be guessed as it is based on something personal. For example, P83 stated:

> "It's secure because I don't think most people would guess that someone would use an old zip code as their PIN *[sic]* and that's minus one zero."

Participants in the security treatment, who have been explicitly told that their 4-digit PIN is insecure, provided more diverse reasons; 41% believed that their 4-digit PIN is "insecure" or "somewhat insecure;" 41% felt it is "somewhat secure" or "secure," and 18% were indecisive.

When asked about the security of their 6-digit PINs, participants perceived it as more secure, ranging from 62% in the no-sub to 73% in the breach treatment. Attributing higher security to 6-digit PINs continues when participants are asked to directly compare the two PINs. As can be seen in Figure 7, over 76% of participants in all the treatments felt their 6-digit PIN is much or slightly more secure than their 4-digit PIN.

For memorability, participants perceive their 4-digit PINs as more memorable. In response to **Q12**, 94% and 95% of participants in neutral and no-sub respectively felt their 4-digit PIN is "somewhat easy" or "easy to remember", with the numbers for security (93%) and upgrade (92%) being only marginally smaller. When directly comparing the two PINs, 52% of participants in upgrade to 63% in security perceive their 4-digit PIN as more memorable. The results for ease of use are similar, with over 60% of participants across treatments indicating their 4-digit PIN is "much easier" or "slightly easier to use" compared to their 6-digit PIN.

Our results indicate that users perceive their shorter 4-digit PINs to be more memorable and easier to use than their 6-digit PINs. While they perceive their 6-digit PINs to be more secure, our guessing results indicate that this is not the case, with 6-digit PINs being sometimes even more insecure.

User Preference Finally, we asked participants which PIN they are more likely to use and their reasons for that. Figure 8 displays these results, with an overall tendency for participants in the neutral (54%), no-sub (58%), and upgrade treatment (58%) to prefer their 4-digit PIN. Participants who have

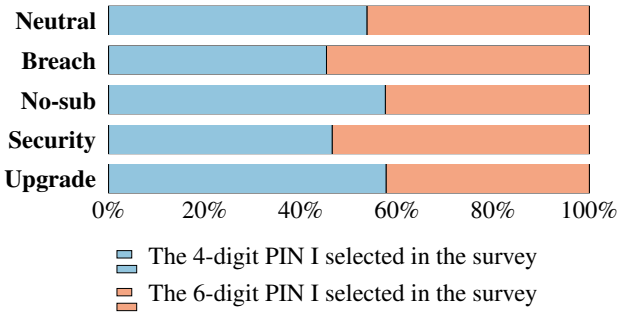


Figure 8: Participants' responses to question **Q20**: "Which of the following are you more likely to use to secure your primary smartphone?"

been warned that their PIN has been breached or that their 4-digit PIN is easily guessable (secure treatment), tend to prefer their 6-digit PIN (54% in both the breach and security treatment). This is further confirmed by a χ^2 test ($p = 0.02$), although the pairwise post-hoc tests did not show significant differences across treatments.

We qualitatively coded free responses describing the reasons for this preference (**Q21**), with the resulting codebook (see Appendix B) revealing that almost all participants who prefer their 6-digit PIN think it is more secure. For instance, P11 said "I feel like the longer PIN is more secure just because it has more digits." Participants who opt for their 4-digit PIN, on the other hand, describe usability benefits, such as being easier or quicker to enter, with P1 saying:

> "I would use it [4-digit PIN] over the other [6-digit PIN] because it is shorter and quicker. I don't worry about anyone getting into my phone."

Some participants also prefer their 4-digit PIN because they believe that the security it offers is sufficient or they are not worried, with P43 stating:

> "I do not keep secure information on my smart phone. Therefore, I am not too concerned about security, and as a result consider the four digit PIN *[sic]* easier to remember and to utilize."

These results highlight the general misconception users have in terms of 6-digit PINs *always* offering an increased level of security in comparison to 4-digit PINs. Often, the reasoning users have when deciding against a 4-digit PIN in favor of a digit 6-PIN may be false. Based on our security analysis, system designers should carefully consider if the marginal security benefits of 6-digit PINs over 4-digit PINs outweigh their usability drawbacks before requiring upgrades.

7 Discussion

In this paper, we analyze the security of "upgraded" 6-digit PINs from 4-digit PINs for smartphone unlocking. We consider different circumstances of the upgrade and its impact on 6-digit PINs, including, and perhaps most relevantly, when a smartphone is upgraded with a new authentication policy. We find that 6-digit PINs are not significantly different from 4-digit PINs in terms of security, confirming prior work [32, 33], and that security-oriented "upgrade" messages slightly improve security. However, when an attacker has knowledge of the 4-digit PIN used prior to the upgrade, the attacker's performance is greatly increased, and the device upgrade scenario leads to the most easily guessed 6-digit PINs.

In the rest of this section, we discuss the implications of these results and offer recommendations that can improve the security of user-selected PINs on mobile devices.

Misconception vs. Preference Similar to prior work on PINs [32, 33], we find that user-selected 6-digit PINs are not significantly different from 4-digit PINs in terms of security. In fact, when a simulated attacker is making up to 10 guesses (the upper limit after which iOS devices block further access), 6-digit PINs are often more insecure than 4-digit PINs. A similar phenomenon is observed for Android unlock patterns by Aviv et al. [7] where a larger grid size does not necessarily increase the security of selected patterns. At the same time, our qualitative results indicate a false sense of security when using a 6-digit PIN, where some participants believe that a 6-digit PIN is more secure in this context simply because it is longer. At the same time, though, most participants would prefer a 4-digit PIN when considering usability criteria, such as memorability and ease of use.

We believe that it is important to address the misconceptions of longer 6-digit PINs being strictly better than 4-digit PINs by not solely promoting 6-digit PINs during mobile device setup. Such efforts could help users better align priorities for usability *and* security. Moreover, if developers are reluctant to recommend 4-digit PINs, a relatively small blocklist (just 27 PINs) would be sufficient to ensure selection of 6-digit PINs that are more difficult to guess within the 10–30 attempt range [32, 33]. However, targeted blocklists may lead to worse security outcomes when selecting 6-digit PINs.

Side Effects of Blocking PIN Subsequences Blocklists have been shown to improve the security of passwords [28, 42, 44, 53], PINs [14, 30, 33], Android unlock patterns [35], and LG Knock Codes [39], and as such, we wanted to explore how blocking subsequences of participants' 4-digit PINs impacts the security of 6-digit PINs. Counter intuitively, the 6-digit PINs selected with the no-sub blocklist led to the most easily guessable 6-digit PINs, when considering the untargeted attacker model. While these PINs were more secure against a targeted attacker, the general insecurity would suggest that such specific interventions that involve the 4-digit PIN may result in poor choices, as compared to simply nudging users with respect to security. Future work can explore how other blocklists, beyond those that prohibit common choices or subsequences during upgrades impact security and usability.

Security Communication During PIN Selection Prior research on passwords [20] has shown that users select related passwords across different sites. Similar to studies on password security [20, 36, 50], we find that a targeted attacker who knows a user's previously selected 4-digit PIN can leverage this knowledge to guess their 6-digit PIN. However, forcing users to create a 6-digit PIN that is completely unrelated to their 4-digit PIN is not a solution; we saw that it may cause frustration and ultimately make users select common, more insecure 6-digit PINs. What proved to be beneficial is priming participants to select secure PINs, similar to prior work showing that clearly communicating risks can increase the effectiveness of password reset emails [27]. Similar communication can be used to increase the security of user-selection of PINs on mobile devices, as recommended by Bailey et al. [11] for Signal PINs. Specifically, PIN selection messages could consider informing users about important data on their devices and how a secure PIN is fundamental for protection of this data [1]. This is a promising area of future research.

Authentication "Upgrading" Policies Just like password policies requiring frequent and unnecessary password changes have proven detrimental to security [18, 25, 42], our results indicate that forcing users to upgrade from 4- to 6-digit PINs does not necessarily improve the security, especially in a targeted attack scenario. Thus, policies requiring rotations of PINs or upgrading of PIN length likely have limited security benefits. Instead, policies should encourage a single selection of an authentication, be it a 4-digit or 6-digit PIN, that is primed for security, rather than unnecessarily forcing an upgrade. Where upgrades are necessary, users should be encouraged to secure their seemingly obsolete 4-digit PINs as our targeted attacker results indicate that an attacker greatly benefits from knowledge of a user's 4-digit PIN when guessing their 6-digit PIN. Moreover, as 4-digit PINs are perceived as more usable and have similar security to 6-digit PINs in the throttled attacker setting, encouraging more secure 4-digit PIN use in policies may lead to much better security outcomes.

8 Conclusion

Through an online user study ($n = 1010$), we investigated how users "upgrade" from 4-digit to 6-digit PINs under various conditions, and its impact on security. In an online attack where the attacker is limited in the number of guesses they can make (10–30), we found that 6-digit PINs only marginally improve security, and are sometimes even more easily guessed compared to 4-digit PINs (confirming prior work). While "upgrades" that communicated "security threats" to users marginally improved the security of 6-digit PINs, we also found that attackers that know a user's previously selected 4-digit PIN performed significantly better at guessing their 6-digit PIN. Our analysis suggests that the small security benefit of 6-digit PINs may not be worth the usability costs they incur. System designers should therefore carefully consider this before upgrading users from 4- to 6-digit PINs. If upgrades occur, users should be encouraged to protect their previous 4-digit PINs as they can be used to predict their 6-digit PINs.

Acknowledgments

We thank Olivia Morkved for her help. We also thank Katharina Krombholz for shepherding this paper, as well as 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. This research was further funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA – 390781972.

References

[1] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. "... 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 *Proc. SOUPS*, 2017.

[2] Daniel Amitay. Most Common iPhone Passcodes, June 2011. http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes.

[3] Panagiotis Andriotis, George Oikonomou, Alexios Mylonas, and Theo Tryfonas. A Study on Usability and Security Features of the Android Pattern Lock Screen. *Information and Computer Security*, 24(1):53–72, March 2016.

[4] Panagiotis Andriotis, Theo Tryfonas, and George Oikonomou. Complexity Metrics and User Strength Perceptions of the Pattern-Lock Graphical Authentication Method. In *Proc. HAS*, 2014.

[5] Panagiotis Andriotis, Theo Tryfonas, George Oikonomou, and Can Yildiz. A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks. In *Proc. WiSec*, 2013.

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

[7] Adam J. Aviv, Devon Budzitowski, and Ravi Kuber. Is Bigger Better? Comparing User-Generated Passwords on 3x3 vs. 4x4 Grid Sizes for Android's Pattern Unlock. In *Proc. ACSAC*, 2015.

[8] Adam J. Aviv, John T. Davin, Flynn Wolf, and Ravi Kuber. Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Proc. ACSAC*, 2017.

[9] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. Smudge Attacks on Smartphone Touch Screens. In *Proc. WOOT*, 2010.

[10] Adam J. Aviv, Flynn Wolf, and Ravi Kuber. Comparing Video Based Shoulder Surfing with Live Simulation and Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Proc. ACSAC*, 2018.

[11] Daniel V. Bailey, Philipp Markert, and Adam J. Aviv. "I have no idea what they're trying to accomplish:" Enthusiastic and Casual Signal Users' Understanding of Signal PINs. In *Proc. SOUPS*, 2021.

[12] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. Counting Clicks and Beeps: Exploring Numerosity Based Haptic and Audio PIN Entry. *Interacting with Computers*, 24(5):409–422, July 2012.

[13] Joseph Bonneau. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *Proc. IEEE S&P*, 2012.

[14] Joseph Bonneau, Sören Preibusch, and Ross Anderson. A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs. In *Proc. FC*, 2012.

[15] Daniel Buschek, Alexander De Luca, and Florian Alt. Improving Accuracy, Applicability and Usability of Keystroke Biometrics on Mobile Touchscreen Devices. In *Proc. CHI*, 2015.

[16] Maria Casimiro, Joe Segel, Lewei Li, Yigeng Wang, and Lorrie Faith Cranor. A Quest for Inspiration: How Users Create and Reuse PINs. In *Proc. WAY*, 2020.

[17] Claude Castelluccia, Markus Dürmuth, and Daniele Perito. Adaptive Password-Strength Meters from Markov Models. In *Proc. NDSS*, 2012.

[18] Sonia Chiasson and Paul C. Van Oorschot. Quantifying the Security Advantage of Password Expiration Policies. *Designs, Codes and Cryptography*, 77(2–3):401–408, December 2015.

[19] Nik Cubrilovic. RockYou Hack: From Bad To Worse, December 2009. https://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/.

[20] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The Tangled Web of Password Reuse. In *Proc. NDSS*, 2014.

[21] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. Now You See Me, Now You Don't: Protecting Smartphone Authentication from Shoulder Surfers. In *Proc. CHI*, 2014.

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

[23] Timothy J. Forman and Adam J. Aviv. Double Patterns: A Usable Solution to Increase the Security of Android Unlock Patterns. In *Proc. ACSAC*, 2020.

[24] Kristen K. Greene, Melissa A. Gallagher, Brian C. Stanton, and Paul Y. Lee. I Can't Type That! P@$$w0rd Entry on Mobile Devices. In *Proc. HAS*, 2014.

[25] Hana Habib, Pardis Emami Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. User Behaviors and Attitudes Under Password Expiration Policies. In *Proc. SOUPS*, 2018.

[26] 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 *Proc. SOUPS*, 2014.

[27] Jun Ho Huh, Hyoungshick Kim, Swathi S.V.P. Rayala, Rakesh B. Bobba, and Konstantin Beznosov. I'm Too Busy to Reset My LinkedIn Password: On the Effectiveness of Password Reset Emails. In *Proc. CHI*, 2017.

[28] Patrick Kelley, Saranga Kom, Michelle L. Mazurek, Rich Shay, Tim Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio López. Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. In *Proc. IEEE S&P*, 2012.

[29] Hassan Khan, Jason Ceci, Jonah Stegman, Adam J. Aviv, Rozita Dara, and Ravi Kuber. Widely Reused and Shared, Infrequently Updated, and Sometimes Inherited: A Holistic View of PIN Authentication in Digital Lives and Beyond. In *Proc. ACSAC*, 2020.

[30] Hyoungshick Kim and Jun Ho Huh. PIN Selection Policies: Are They Really Effective? *Computers & Security*, 31(4):484–496, June 2012.

[31] Marte Løge, Markus Dürmuth, and Lillian Røstad. On User Choice for Android Unlock Patterns. In *Proc. EuroUSEC*, 2016.

[32] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs. In *Proc. IEEE S&P*, 2020.

[33] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. On the Security of Smartphone Unlock PINs. *ACM Transactions on Privacy and Security*, 24(4):30:1–30:36, November 2021.

[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. Usability and Security of Text Passwords on Mobile Devices. In *Proc. CHI*, 2016.

[35] Collins W. Munyendo, Miles Grant, Philipp Markert, Timothy J. Forman, and Adam J. Aviv. Using a Blocklist to Improve the Security of User Selection of Android Patterns. In *Proc. SOUPS*, 2021.

[36] Bijeeta Pal, Tal Daniel, Rahul Chatterjee, and Thomas Ristenpart. Beyond Credential Stuffing: Password Similarity Models using Neural Networks. In *Proc. IEEE S&P*, 2019.

[37] Athanasios Papadopoulos, Toan Nguyen, Emre Durmus, and Nasir Memon. IllusionPIN: Shoulder-Surfing Resistant Authentication Using Hybrid Images. *IEEE Transactions on Information Forensics and Security*, 12(12):2875–2889, December 2017.

[38] Elissa M. Redmiles, Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek. A Summary of Survey Methodology Best Practices for Security and Privacy Researchers. Tech report, 2017.

[39] Raina Samuel, Philipp Markert, Adam J. Aviv, and Iulian Neamtiu. Knock, Knock. Who's There? On the Security of LG's Knock Codes. In *Proc. SOUPS*, 2020.

[40] Florian Schaub, Ruben Deyhle, and Michael Weber. Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms. In *Proc. MUM*, 2012.

[41] Stuart Schechter and Joseph Bonneau. Learning Assigned Secrets for Unlocking Mobile Devices. In *Proc. SOUPS*, 2015.

[42] Richard Shay, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Alain Forget, Saranga Komanduri, Michelle L. Mazurek, William Melicher, Sean M. Segreti, and Blase Ur. A Spoonful of Sugar?: The Impact of Guidance and Feedback on Password-Creation Behavior. In *Proc. CHI*, 2015.

[43] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Proc. SOUPS*, 2010.

[44] Joshua Tan, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Practical Recommendations for Stronger, More Usable Passwords Combining Minimum-Strength, Minimum-Length, and Blocklist Requirements. In *Proc. CCS*, 2020.

[45] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. In *Proc. CCS*, 2013.

[46] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. SwiPIN: Fast and Secure PIN-Entry on Smartphones. In *Proc. CHI*, 2015.

[47] Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. Honey, I Shrunk the Keys: Influences of Mobile Devices on Password Composition and Authentication Performance. In *Proc. NordiCHI*, 2014.

[48] Emanuel von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. Easy to Draw, but Hard to Trace?: On the Observability of Grid-based (Un)Lock Patterns. In *Proc. CHI*, 2015.

[49] Emanuel von Zezschwitz, Malin Eiband, Daniel Buschek, Sascha Oberhuber, Alexander De Luca, Florian Alt, and Heinrich Hussmann. On Quantifying the Effective Passsword Space of Grid-Based Unlock Gestures. In *Proc. MUM*, 2016.

[50] Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, and Gang Wang. The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services. In *Proc. CODASPY*, 2018.

[51] Ding Wang, Qianchen Gu, Xinyi Huang, and Ping Wang. Understanding Human-Chosen PINs: Characteristics, Distribution and Security. In *Proc. ASIACCS*, 2017.

[52] Ding Wang, Zijian Zhang, Ping Wang, Jeff Yan, and Xinyi Huang. Targeted Online Password Guessing: An Underestimated Threat. In *Proc. CCS*, 2016.

[53] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. In *Proc. CCS*, 2010.

Appendix

A Survey Instrument

Agenda

On the next page, you will have a chance to practice entering a 4-digit PIN before proceeding with the rest of this survey, where we will ask you to select your own 4-digit PIN that you would use to unlock your primary smartphone.

Enter 4 digits

PIN pad as shown in Figure 1

Instructions

For this survey, you will be asked to create a 4-digit PIN that you would likely use to unlock your primary smartphone. You will need to recall this PIN later in the survey, so choose something that is as secure and memorable as you may use on your primary smartphone. We ask that you **DO NOT** write down your PIN or use other aids to help you remember.

I understand that I will be asked to create a 4-digit PIN that I would use to unlock my primary smartphone.

○ I understand these instructions

I understand that I should not write down my 4-digit PIN or use other aids to assist in the survey.

○ I understand these instructions

Create a 4-digit PIN

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

PIN pad as shown in Figure 1

Questions about 4-digit PIN

Q1 Many people have strategies when selecting a PIN. What strategy did you use to select your 4-digit PIN?
Answer: _____

Q2 If you were to use a 4-digit PIN on your primary smartphone, would use the 4-digit PIN you selected in this survey or would you choose a different one?
○ Yes, I would use the 4-digit PIN I created here on my primary smartphone.
○ No, I would not use the 4-digit PIN I created here but instead would create a new one to use on my primary smartphone.
○ Unsure, I may or may not use the 4-digit PIN I created here on my primary smartphone.

Q3 Please explain why you would or would not use the 4-digit PIN you selected here on your primary smartphone.
Answer: _____

Enter Device Information

Q4 What is the operating system of your primary smartphone?
○ Android ○ iOS (iPhone) ○ Other ○ Prefer not to say

Q5 Do you use any of the following biometrics to unlock your primary smartphone? (Select all that apply)
☐ Fingerprint ☐ Face ☐ Iris ☐ Other biometric
☐ I do not use a biometric

*If participant indicated they use a biometric in **Q5**:*

Q5a How do you unlock your smartphone, if your biometric fails or when you reboot your smartphone?
○ Pattern ○ 4-digit PIN ○ 6-digit PIN ○ PIN of other length
○ Alphanumeric password ○ Other unlock method ○ None

*If participant indicated they do not to use a biometric in **Q5**:*

Q5b What screen lock do you use to unlock your primary smartphone?
○ Pattern ○ 4-digit PIN ○ 6-digit PIN ○ PIN of other length
○ Alphanumeric password ○ Other unlock method ○ None

Instructions

Neutral/No-sub: To continue the study, now you must select a 6-digit PIN.
Breach: Imagine someone learned your 4-digit PIN and to protect your smartphone, now you must select a 6-digit PIN.
Security: Research has shown that the 4-digit PIN you selected is insecure and can be easily guessed. To continue the study, now you must select a 6-digit PIN.
Upgrade: Imagine you are upgrading your smartphone that requires PINs longer than 4-digits, and so now you must select a 6-digit PIN.

On the next page, you will create a 6-digit PIN that you would likely use to unlock your primary smartphone. To set your 6-digit PIN, you will first confirm your 4-digit PIN and then select the 6-digit PIN.

Re-enter your 4-digit PIN

PIN pad as shown in Figure 1

Create a 6-digit PIN

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

PIN pad as shown in Figure 3

Questions about 6-digit PIN

Q6 Many people have strategies when selecting a PIN. What strategy did you use to select your 6-digit PIN?
Answer: _____

Q7 Is your 6-digit PIN related to your 4-digit PIN?
○ Yes ○ Somewhat ○ No ○ Prefer not to answer

Q8 If you were to use a 6-digit PIN on your primary smartphone, would use the 6-digit PIN you selected in this survey or would you choose a different one?
○ Yes, I would use the 6-digit PIN I created here on my primary smartphone.
○ No, I would not use the 6-digit PIN I created here but instead would create a new one to use on my primary smartphone.
○ Unsure, I may or may not use the 6-digit PIN I created here on my primary smartphone.

Q9 Please explain why you would or would not use the 6-digit PIN you selected here on your primary smartphone.
Answer: _____

*If participant indicated their 4- and 6-digit PINs are related in **Q7**:*

Q9a Please explain how your 6-digit PIN and your 4-digit PINs are related.
Answer: _____

Questions about 4-digit PIN

We now want to ask you a few questions about your selected 4-digit PIN. It is displayed below for your reference.

4-digit PIN chosen earlier

Q10 I feel the 4-digit PIN I chose is:
○ Insecure ○ Somewhat insecure ○ Neither secure nor insecure
○ Somewhat secure ○ Secure

Q11 Please explain why you consider the 4-digit PIN you selected as secure or insecure.
Answer: _____

Q12 I feel the 4-digit PIN I chose is:
○ Hard to remember ○ Somewhat hard to remember
○ Neither easy nor hard to remember
○ Somewhat easy to remember ○ Easy to remember

Q13 I feel the 4-digit PIN I chose is:
○ Hard to use ○ Somewhat hard to use
○ Neither easy nor hard to use
○ Somewhat easy to use ○ Easy to use

Q14 Select agree as the answer to this question.
○ Strongly disagree ○ Disagree ○ Neither agree or disagree
○ Agree ○ Strongly agree

Instructions

On the next page, you will be asked to recall the **6-digit** PIN that you selected earlier in the survey.

Re-enter your 6-digit PIN

PIN pad as shown in Figure 3

Questions about 6-digit PIN

We now want to ask you a few questions about your selected 6-digit PIN. It is displayed below for your reference.

6-digit PIN chosen earlier

Q15 I feel the 6-digit PIN I chose is:
○ Insecure ○ Somewhat insecure ○ Neither secure nor insecure
○ Somewhat secure ○ Easy to secure

Q16 Please explain why you consider the 6-digit PIN you selected as secure or insecure.
Answer: _____

Q17 I feel the 6-digit PIN I chose is:
○ Hard to remember ○ Somewhat hard to remember
○ Neither easy nor hard to remember
○ Somewhat easy to remember ○ Easy to remember

Q18 I feel the 6-digit PIN I chose is:
○ Hard to use ○ Somewhat hard to use
○ Neither easy nor hard to use
○ Somewhat easy to use ○ Easy to use

Q19 What is the shape of a blue ball?
○ Red ○ Blue ○ Square ○ Round

Comparison Questions

Q20 Which of the following are you more likely to use to secure your

primary smartphone?
○ The 4-digit PIN I selected in the survey
○ The 6-digit PIN I selected in the survey

Q21 Please explain why you would use your preferred choice above to secure your primary smartphone.
Answer: _____

Q22 Of the two PINs you created, which do you think is more secure?
○ My 6-digit PIN is much more secure
○ My 6-digit PIN is slighty more secure
○ My 4-digit and 6-digit PINs are equally secure
○ My 4-digit PIN is slighty more secure
○ My 4-digit PIN is much more secure

Q23 Of the two PINs you created, which do you think is easier to remember?
○ My 6-digit PIN is much easier to remember
○ My 6-digit PIN is slighty easier to remember
○ My 4-digit and 6-digit PINs are equally easy to remember
○ My 4-digit PIN is slighty easier to remember
○ My 4-digit PIN is much easier to remember

Q24 Of the two PINs you created, which do you think is easier to use?
○ My 6-digit PIN is much easier to use
○ My 6-digit PIN is slighty easier to use
○ My 4-digit and 6-digit PINs are equally easy to use
○ My 4-digit PIN is slighty easier to use
○ My 4-digit PIN is much easier to use

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 best describes you?
○ Male ○ Female ○ Non-Binary ○ Prefer to Self-Describe
○ Prefer not to say

D3 What is your dominant hand?
○ Left handed ○ Right handed ○ Ambidextrous ○ I do not know
○ Prefer not to say

D4 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

D5 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 Qualitative Codes

Using the method described in Section 4, we coded the answers to questions **Q1**, **Q3**, **Q6**, **Q9**, **Q9a**, **Q11**, **Q16**, and **Q21**. Below, we list all resulting codes and subcodes along with their counts.

- **easy-to-remember (406)**
- **personal (315)**
  unlikely (85), birthday (36), phone-number (29), easy (28), unknown (16), address (13), favorite-number (7), pet (6), name (5), anniversary (5), school (4), childhood (4), lucky (3), pin (3), combination (3), initials (3), tv (2), zip-code (2), number (2), word (2), parent (1), drivers-license (1), ssn (1), music (1), atm (1), favorite-letter (1), hotel-room (1), song (1), likely (1), sports (1), work (1), credit-card (1), family (1)
- **more-secure (248)**
  harder-to-guess (61), harder-to-observe (13)
- **difficult-to-guess (219)**
  6digits (1), shoulder-surf (1)
- **easier (186)**
  easier-to-remember (86), easier-to-enter (64), easy-for-others (1), pattern (1)
- **easy-to-guess (174)**
  shoulder-surf (9)
- **date (158)**
  birthday (107), year (12), month-day (6), birth-year (5), day-month (3), year-year (3), history (2), month-year (2), today (2), anniversary (2), holiday (1), month-day-year (1), month (1), day-year (1)
- **random (131)**
- **security (106)**
- **keypad-pattern (104)**
  non-specific (34), middle (8), corners (8), diagonal (8), vertical (6), line (3), center (2), right (2), x (2), row (2), non-specific (1), shape (1), tetris (1), across (1), diamond (1), L-shape (1), y (1), rectangle (1)
- **personal-info (94)**
  birthday (35), date (17), phone-number (4), childhood (3), address (1), name (1), pet (1)
- **same-numbers (73)**
  start (24), reverse (7), repetition (4), start-end (3), end (3), date (1), opposite (1)
- **quicker-to-enter (73)**
- **more-secure-longer (63)**
- **previously-used (62)**
  pin (1)
- **hide-real-pin (55)**
- **easy-to-enter (50)**
- **good-enough (47)**
- **pattern (45)**
- **would-not-use (45)**
- **not-personal (44)**
- **simple (41)**
- **no-reuse (38)**
- **changed-4-digit (31)**
  append (14), prepend (1)
- **currently-used (30)**
- **same-as-before (28)**
- **sufficient (27)**
- **same-strategy (26)**
  humor (1), state (1)
- **unique (26)**
- **word (26)**
  name (10)
- **other-auth-method (24)**
- **repetition (23)**
- **used-to (20)**
- **same-pattern (21)**
  vertical (2), birthday (1), mirror (1)
- **too-short (20)**
- **not-worried (19)**
- **not-previously-used (18)**
- **basic (15)**
- **easy-to-use (14)**
- **no-personal-info (14)**
- **unconcerned (14)**
- **longer (12)**
- **unsure (10)**
- **privacy (8)**
- **breach (8)**
- **humor (7)**
  word (1)
- **required (7)**
- **shorter (7)**
- **trust (7)**
- **no-change (6)**
- **none (6)**
- **numeric-pattern (6)**
- **same-structure (4)**
- **study-specific (4)**
- **current-pin (3)**
- **number (3)**
  13 (2), 14 (1)
- **mnemonic (2)**
- **same (2)**
- **words (2)**
- **known-by-others (1)**
- **math (1)**
- **more-familiar (1)**
- **memorize (1)**
- **safety (1)**