Nudging Bank Account Holders Towards More Secure PIN Management

Andreas Gutmann[1], Karen Renaud[2], Melanie Volkamer[1]
Technische Universität Darmstadt[1], Germany
University of Glasgow[2], UK

Abstract

The memorability of PINs is an enduring security issue. This is especially pertinent in the context of banking, where technical systems evolve more slowly than in other contexts (e.g. many mobile phone operating systems have adopted alternative authentication mechanisms). Banking customers who struggle to memorise all their PINs often record them, sometimes insecurely, flying in the face of advice from their banks. Banks respond to memorisation difficulties by permitting customers to change their PINs. The reality is that both recording and changing unwittingly weakens the mechanism by increasing predictability. Yet trying to forbid these coping strategies is futile. It is far better to acknowledge the prevalence of such behaviours and to try to nudge people towards more secure PIN management. In this paper, we suggest a way of achieving this.

1. Introduction

Personal Identification Numbers, or PINs, have been used for decades to secure access to customers banking accounts. Banks issue system-generated random PINs to their customers and rely on them to keep it safe. The only advised PIN management option is committing it to memory.

A bank customer receiving a new PIN has other options, in addition to memorising the PIN: first to change it and second to record it (see Fig 1). Changing clearly weakens the mechanism because humans are incapable of randomness [1], and this propensity will extend to PIN choice. Recording the PIN exacerbates the danger posed by theft, even more so if the record is carried with the banking card itself or recorded somewhere obvious.

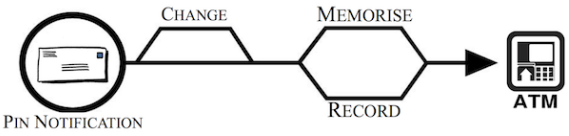

Figure 1. PIN management Options when issued with a new PIN: Change (or not) then Memorise or Record

There is plenty of evidence to show that many people choose insecure options, either changing or recording their PINs [2]. This is most likely because memorising all their randomly issued PINs and passwords is impossible.

Forbidding insecure behaviours is clearly futile. Since people are recording and changing despite being advised not to do so, they are equally likely to disregard prohibitions. A more reasonable alternative is to accept that such coping behaviours exist as the inevitable consequence of memorisation difficulties. This stance leads us to propose providing PIN holders with advice in order to *nudge* them towards more secure variations of changing and recording.

The contribution of this paper is to propose advice in the form of a PIN management leaflet derived from the findings of previous research, then to report on an evaluation of the leaflet. We conclude by suggesting the next iteration of the leaflet based on the results of our evaluation.

2. Literature Review

Previous research has focused on helping people to learn randomly-generated PINs. Schechter and Bonneau [4], for example, proposed and tested two methods. The first required the person to login with a self-chosen PIN. A second PIN then slowly revealed itself on the screen. The person had to type it in to complete logging in. The gradual appearance of the second PIN motivated the person to type in the PIN from memory before full appearance. The second method exploited visual memory by deterministically scrambling the PIN pad. The person logged in with a self-chosen PIN. After each number was entered, the PIN pad scrambled itself deterministically, i.e. pressing different numbers produced different layouts but the same number sequence always produced the same layout. This procedure was supposed to motivate the person to remember the entry pattern, instead of the individual actual PIN. Thus both methods introduced and attempted to entrench a new PIN, the first committing a distinct number and the second a pattern or shape on the PIN pad. Sadly both methods would require a wholesale change to automated teller machines worldwide and this has not been adopted. The authors suggested that their techniques be deployed on mobile phones.

Huh *et al.* [5] investigated whether chunking could help users to memorise PINs of different lengths. They concluded that PINs of length four were easiest to remember and that PINs of more than four numbers were easier to remember when presented in chunks of

length up to four, e.g. PINs of length eight performed best when presented as three chunks of length 2-2-4.

Some researchers have proposed assistance to help people with their PINs. For example, Renaud and Smith [6] proposed a mechanism called 'Jiminy' for securely recording PINs. Jiminy is a software tool that embeds a PIN into a grid of numbers superimposed onto an image. The grid was printed and could be publicly displayed; a coloured template, which could be kept secure, was used to reveal the PIN. This scheme suffered from being rather clumsy, requiring printouts and plastic templates to be secured.

Spydeberg Sparebank came up with an alternative mechanism which assists customers by providing a credit-card sized cut-out. The customer is instructed to write the PIN in the grid, using a particular combination of colours and positions. The scheme is insecure, since people demonstrate predictability, often using the top left-hand corner of such a grid as an anchor [7].

3. Secure Retention

Renaud and Volkamer [3] outlined the mental models underlying the behaviours of bank customers with respect to PIN management. Based on this insight, they suggested advice that banks could provide to their customers when issuing a new PIN in order to encourage more secure retention. We provide a brief summary of their advice here.

3.1 Memorisation Advice

Committing a new PIN to memory is the advisable course of action. Customers should be provided with a number of different strategies and methods of memorising their PINs. The most popular memorisation strategies are (1) visualisation, i.e. the shape of your finger moving from one number to the next one when entering a PIN, (2) association of numbers to dates, or other numbers that one knows, and (3) to develop a story using the numbers in the PIN.

3.2 Recording Advice

Participants do record their PINs despite this practice being proscribed by most banks [3, 8]. When it is clear that a behaviour cannot be feasibly forbidden, other strategies need to be considered. An alternative is to assist customers who prefer to record their PINs so that they do it as securely as possible. Secure recording options using password managers and explaining how to 'encrypt' the PIN by applying an algorithm (e.g. adding or subtracting 1111 before recording) might be helpful.

3.3 Changing Advice

Many banks permit customers to change their PINs. To mitigate against popular (and predictable) PIN choices, as described by Bonneau *et al.* [2], guidance should be provided. A list of predictable PINs could be provided, with advice that these should be avoided. Examples are 1234, 2580 and 1111 [8].

4. PIN leaflet

Taking the advice listed in Section 2, we developed an initial PIN leaflet depicted in Figure 2. The goal was to keep the advice as simple and accessible as possible. The leaflet consists of three sides: a covering page and two content pages. We placed the memorisation advice on the first content page as it is the most secure and thus recommended option. Advice regarding the recording of PINs is listed second and advice related to choosing new PINs is displayed on the last page. We provided descriptive images where appropriate.

The PIN 7389 was used to illustrate several different approaches to keep consistency. We added the label 'Example' to the 'Use Secret Recipe' advice to avoid everyone using exactly the same encryption algorithm. Lastly we included a warning picture regarding shoulder surfers.

5. Study

We conducted a survey to evaluate the leaflet. We were particularly interested in whether (1) the provided advice was perceived to be useful and (2) whether participants would consider utilising the provided advice, as well as (3) identifying possible improvements to the leaflet.

5.1 Design

The use and memorisation of PINs is a sensitive subject with respect to the participants' privacy. We were concerned that they might be reluctant to provide honest and candid responses if they were afraid this information could somehow compromise their own bank account's security. Therefore we chose to conduct an online survey and refrain from collecting demographic or identifying data.

The participants were recruited on CrowdFlower and informed that they were helping us to design a leaflet to be used by banks when they issue new PINs to their customers.

5.2 Apparatus

The survey provided an illustration of the leaflet, as described in Section 3 and depicted in Figure 2. Participants were first asked to answer two multiple

choice questions: The first question asked how they usually act when they receive a new PIN. After examining the leaflet, the second question asked which advice they considered useful. Finally, we asked whether the leaflet would make them reconsider what they usually do with new PINs. Finally we posed three questions eliciting free-text responses on what ought to be added or removed from the leaflet and what they really liked about it.

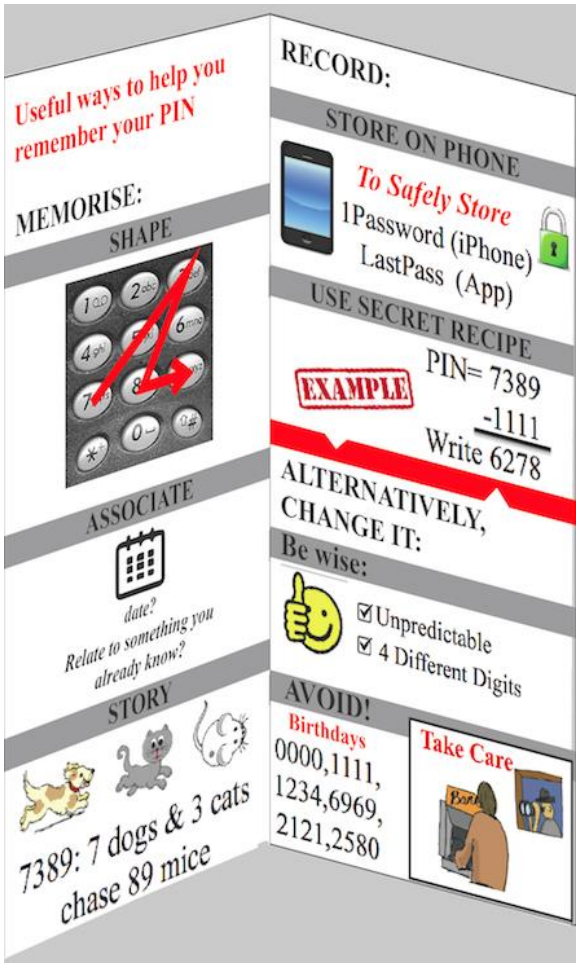

Figure 2. The second and the third panel of the PIN leaflet. The first panel, a covering page, is not displayed

5.3 Results

We collected a total of 200 responses from CrowdFlower. Six participants were excluded because their responses did not make sense. Another participant was excluded because, most likely due to an encoding error, we were unable to read their responses to the last three questions.

156 of the remaining 193 participants usually attempted to memorise new PINs. 73 relied solely on their memory. 29 respondents changed their PINs to a more memorable one before memorising. 64 participants recorded their PIN. 13 of these reported that they relied solely on recording, whereas 15 changed their PINs before recording. 24 participants commented that their action would depend on the issued PIN and 35 deploy a combination of memorisation and recording. These responses are summarised in Table 1.

Table 1. How do the participants usually proceed when they receive a new PIN?

Number of Participants who	Rely On	Solely Rely On	Change First
Memorise	156	73	29
Record	64	13	15
Memorise and Record	35		
Depends on PIN	24		

After examining the leaflet, 128 participants found the memorising advice to be useful (which is in line with memorisation being the most used method of handling a new PIN). 51 considered the recording advice useful and 58 liked the changing advice. (Multiple answers were possible.) 25 participants found the advice not useful and 15 of these considered that they did not require any advice. In terms of whether the leaflet made them rethink what they usually do, 61 participants agreed. 34 and 4 answers were "maybe" and “I don't know”, respectively. 94 participants would not change their usual practices, with 67 claiming to be content with their current PIN management strategies. These responses are summarised in Tables 2 and 3.

Table 2. Which advice in the leaflet did the participants find useful?

	Number of Participants
Memorisation	128
Recording	51
Changing	58
Nothing	10
Don't need advice	15

Table 3. Would the leaflet make the participants reconsider what they usually do with new PINs?

	Number of Participants
Rethink	61
Maybe	34
Don’t Know	4
Not Interested	67
No	27

We categorised the free text responses into three groups: (1) completely positive, (2) mainly positive with some remarks, (3) many remarks or completely negative. Based on these categories, 77 participants were overwhelmingly positive in their responses. 26 of these stated that they would reconsider their usual strategies for managing new PINs, 28 said they were satisfied with their current practice and 14 were noncommittal. 111 gave either two completely positive responses or one completely positive and two mainly positive ones. Of those 111, 33 said the leaflet would influence what they usually did, 37 claimed to be satisfied with their current practice and 20 were noncommittal. Two participants provided many remarks and said that the leaflet would impact their handling of new PINs. Another 3 considered the leaflet to be useless. This is summarised in Table 4.

Table 4. Categorisation of free text responses to the questions of what the participants want to be added or removed and what they really like

	Very Positive	Mainly Positive	Many Remarks
Total Answers	77	111	5
Rethink	26	33	2
Maybe	14	20	-
Happy with what they do	28	37	2
No/Don't know	9	21	1

Within the free text responses, 8 participants particularly enjoyed the provided examples and 14 would have liked more examples, whereas 4 participants stated that some or all of the examples should be removed. 18 people enjoyed the story advice whereas 12 said they ought to be removed from the leaflet. Another 14 responses requested more memorisation strategies.

15 participants indicated that storage on a mobile phone app should be removed for security reasons, opposed to two people who like that suggestion. Another 12 would have liked the secret recipe advice to be more detailed with particular emphasis on not recording PINs in the clear.

Additional advice on how to contact the bank and what to do if they lost their PIN was requested by 5 participants. A new design with more space was requested by 15 respondents and another 8 considered the front page to be superfluous.

6. Discussion

Roughly 50% of the participants stated that they would not be influenced by the leaflet in terms of their usual approach to handling new PINs. This is in line with findings by Renaud and Volkamer [3] that some people are less open to advice in general. This might be because they are satisfied with their current approach. At the same time most participants liked the leaflet (188/193 noted "no" or "only few/minor" changes) in its current form. This suggests that a complete overhaul of the design and content is ill advised. The co-occurrence of both observations indicates that the rejection of the advice by some participants holds even when they are confronted with advice they perceive to be useful. This is no contradiction since participants might have based their rating on the usefulness to an audience other than themselves.

More than 30% of the participants noted that they did rethink their usual behaviour after reading the leaflet, which indicates that the leaflet fulfilled its core purpose. Nonetheless, some improvements to the leaflet are advisable since more than 17% were unsure about whether they would be influenced by it. This is further supported by the fact that only about 40% of the participants did not provide content-related comments.

We conclude that while the current leaflet seems to fulfil its purpose for some stakeholders, others who are seemingly open to advice did not respond to it in the way we anticipated. Hence further improvements and refinements are indicated.

7. Limitations

Questioning people about PIN-related behaviour is a privacy-sensitive task. We conducted our study on CrowdFlower and refrained from asking demographic or identifying questions in order to provide an anonymous environment. An online survey is always reliant on self-report and might sometimes have been performed under time pressure or distraction. Thus we cannot guarantee correctness of our results. However, it does not seem likely that anyone would have been motivated to respond untruthfully. Thus we do not believe this eventuality to be a serious threat to the validity of our findings.

8. Revised and Refined Leaflet

The results of our user study provide several directions for possible improvements to the leaflet. Naturally some contradict each other. Thus we tried to cover common ground behind the comments instead of trying to address each and every individual comment.

There was general agreement that the leaflet's design was too crowded, including indications that the front page was superfluous. We thus removed the front page and thus increased the space for the actual content by 50%.

The next focus was the section containing memorisation strategies. Memorisation was rated

most useful by our participants. Common ground within the remarks was to provide more detailed descriptions, more examples and more memorisation strategies. The inclusion of more descriptions and examples is straightforward. We also included two additional memorisation strategies. The association with words based on letters printed on a PIN pad was recommended by our participants and therefore included. The use of arithmetic in our secret recipe advice was perceived so positively that we decided to include arithmetic as a memorisation strategy of its own.

We allocated the space gained from removing the front page to this section. We thus doubled the size and ended with a less crowded section despite adding content, as can be seen in Figures 3 and 4.

We removed the advice related to the use of password managers on mobile phones. In general, we believe that offering more diverse advice is good practice to cater to a diverse customer base. Unfortunately, in this case, the advice was very rarely perceived to be useful. We felt that the predominant concern of such advice encouraging insecure behaviour could compromise overall trust in the leaflet. We also responded to several remarks that we should insist on people never writing down their PINs in the clear by providing more detailed instructions in the secret recipe advice. The outcome of these changes is displayed in the top part of Figure 5.

The process of providing instructions that were clearer led to a revision of PIN changing advice. We replaced the bullet point style layout and the ill-advised PINs with two simple rules covering the same aspects. Those rules can be seen in the middle part of Figure 5.

Finally we added an advice for people to repeat the strategy chosen for a new PIN several times to fix the PIN in their mind. We also changed the warning to protect PIN entry from the view of shoulder surfers by providing more precise and constructive advice on covering the PIN pad. This advice is on the bottom part of Figures 4 and 5.

For the other side of the leaflet we recommend banks include clear instructions on what to do if a customer loses or forgets their PIN and on how to contact the bank for all PIN-related eventualities.

9. Conclusion

Our goal of this paper was to introduce a leaflet which aims to help banking customers with their PIN management. The idea is that banks would issue the leaflet together with new PINs. We started with a leaflet based on the work of Renaud and Volkamer [3] outlined in Section 3. We evaluated it in an online user study. Our findings, as presented in Section 5, were that while the leaflet did influence about half of the participants, a notable subset of respondents were not fully satisfied and unsure about whether the provided leaflet would influence or help them, or not.

Figure 3. Left-hand Panel of the Revised Leaflet

We revised and refined the leaflet based on our study. We conclude this paper with an updated version of the leaflet in Section 7. As this leaflet was originally based on banking customers' mental models, evaluated in a user study and further refined, we believe that it is getting close to being ready for deployment.

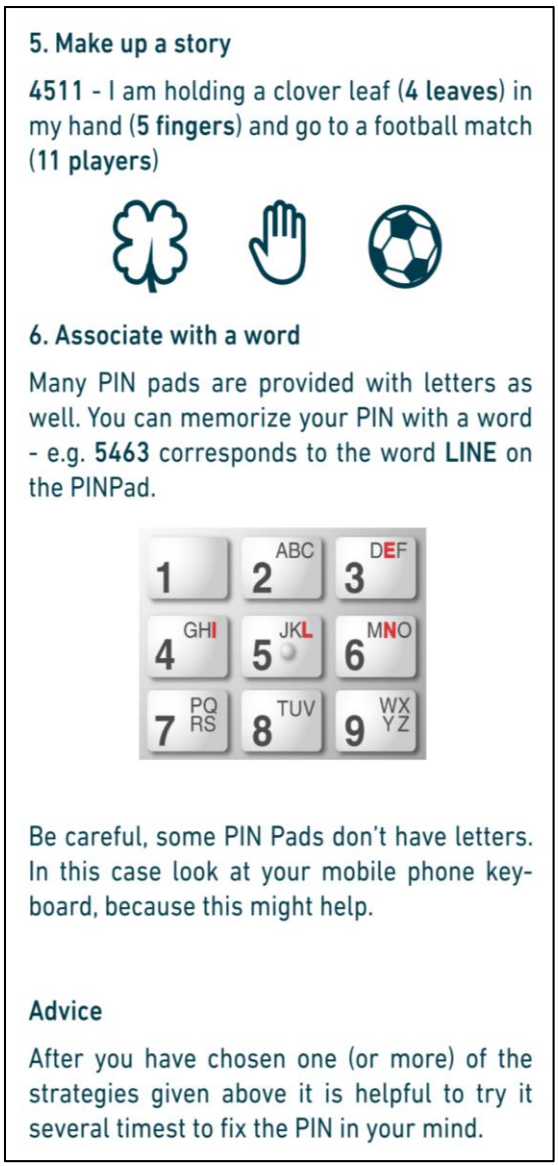

Figure 4. Middle Panel of the Revised Leaflet

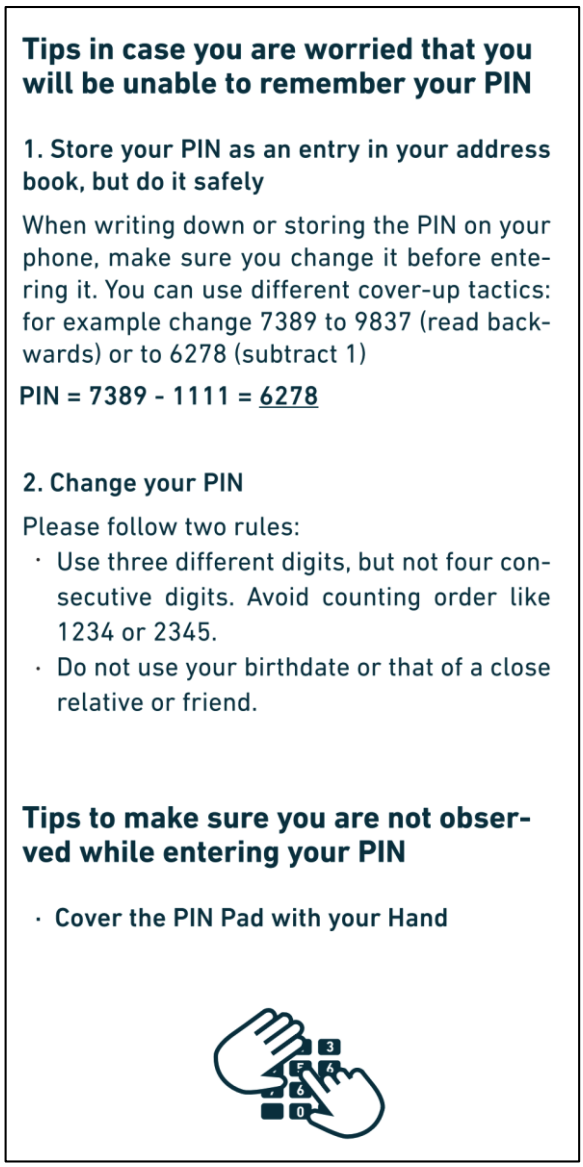

Figure 5. Right-Hand Panel of the Revised Leaflet

10. Future Work

We believe that the revised leaflet is an improvement over the first one. Nonetheless, it would be overly optimistic to infer that further refinements are not required. We thus plan to conduct focus group interviews to evaluate the next iteration. This will give us a more in-depth understanding of the matter and identify further refinements.

Complementary to this work it could be beneficial to investigate whether it is practical to modify the PIN change procedure at ATMs such that, instead of choosing a new PIN, customers can opt for a new randomly generated PIN which is specifically tailored to their preferred memorisation strategy. While this seems to be technically feasible, the adoption thereof by banking customers remains an open question.

Furthermore, it would be interesting to investigate whether modifications of the advice presented in this leaflet can (under certain circumstances) improve memorability of system-generated passwords.

11. References

[1] M. Figurska, M.Stańczyk, and K. Kulesza. Humans cannot consciously generate random numbers sequences: Polemic study. *Medical hypotheses*, 70(1):182-185, 2008.

[2] J. Bonneau, S.Preibusch, and R. Anderson. A birthday present every eleven wallets? The security of customer-chosen banking PINs. In *Financial Cryptography and Data Security*, pages 25-40. Springer, 2012.

[3] K. Renaud and M. Volkamer. Exploring mental models underlying PIN management strategies. In *World Congress on Internet Security (WorldCIS 2015)*, pages 18-23, 2015.

[4] S. Schechter and J. Bonneau. Learning assigned secrets for unlocking mobile devices. In *Symposium on Usable Privacy and Security (SOUPS)*, 2015.

[5] J. H. Huh, M. Bashir, H. Kim, K. Deznosov, and R. B. Bobba. On the memorability of system-generated PINs: Can chunking help? In *SOUPS*, Menlo Park, California, 9-11 July 2014.

[6] K. Renaud and E. Smith. Jiminy: Helping users to remember their passwords. In *Annual Conference of the South African Institute of Computer Scientists and Information Technologists*. SAICSIT'2001, pages 73-80, Pretoria, South Africa, 2001.

[7] P. Andriotis, T. Tryfonas, and G.Oikonomou. Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In *HCI International*, Crete, Greece, June 2014.

[8] N. Berry. PIN Analysis. DataGenetics; http://www.datagenetics.com/blog/september32012/index.html (10 November 2015).

