Exploring Mental Models Underlying PIN Management Strategies

Karen Renaud
School of Computing Science
University of Glasgow
Glasgow, United Kingdom
Email: karen.renaud@glasgow.ac.uk

Melanie Volkamer
Department of Computer Science
Technische Universität Darmstadt
Darmstadt, Germany
melanie.volkamer@cased.de

***Abstract*—PINs have been around for half a century and many insecure PIN-related practices are used. We attempted to mitigate by developing two new PIN memorial assistance mechanisms that we tested in an online study. We were not able to show an improvement in memorability, mostly because people did not use the memorial aids. We realised that a greater insight into PIN Management mental models was needed, in order the better to formulate mitigation approaches. We proceeded to study PIN-related mental models, and we present our findings in this paper. The insights we gained convinced us that security researchers should not presume that people want, or need, our advice or help in any security context; they might well prefer to continue with their usual trusted practices. Yet advice *should* indeed still be offered, for those who do want it, and we make some suggestions about what this advice should look like in the PIN context.**

***Keywords*—PINs, Mental Models, Strategies.**

I. Introduction

A bank customer receiving a new PIN has two primary options: first to memorise the PIN, second to record it. Some banks permit customers to change the PIN before memorising or recording (see Fig 1). The only advised PIN management option is committing it to memory. Changing is clearly unwise because humans are incapable of randomness [10], and this propensity will extend to PIN choice. There is plenty of evidence to show that many people choose the insecure options, changing and recording PINs [4]. This is most likely because memorizing all their randomly issued PINs and passwords is impossible. Researchers previously experimented with recording obfuscated PINs on paper [16] to address this issue but users found it clunky and it was not adopted.

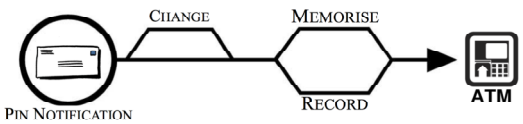

Fig. 1. PIN Management: Three options when issued a new PIN: Change, Memorise or Record.

The availability of more effective PIN memorisation techniques could remove the need for insecure coping strategies. The initial goal of our research, therefore, was to find out whether novel memorisation techniques deduced from literature could make it easier for people to remember their PINs. We carried out an experiment (Study 1) to test the impact of two new memorial assistance mechanisms (Section II). There was, unfortunately, no improvement in PIN retention. The free text responses made it clear that almost half of the participants did not even use our memorial mechanisms, preferring to stick with their usual memorisation strategies. We concluded that if we wanted to offer advice, we needed first to understand extant PIN management strategies.

We carried out surveys (Study 2) to explore these mental models (Section III). Based on our findings, we deduced mental models underlying PIN management (Section IV) and suggest PIN management advice that banks could include with PIN notifications based on the mental models we derived (Section V).

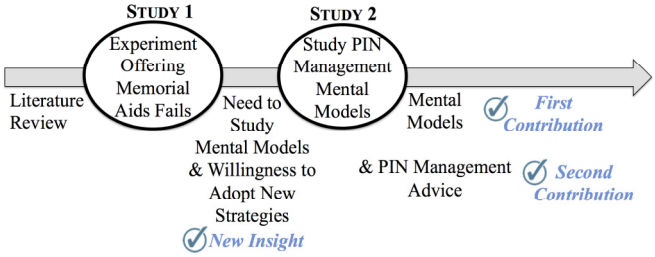

Fig. 2. Research approach, structure of this paper, and results.

The main contributions of this paper are:

- Firstly, to offer an insight into the mental models underlying PIN management choices.
- Secondly, suggestions about advice banks could issue, together with PIN notifications, in order to help users to manage their PINs more securely.

Furthermore, we gained a new insight into the security researchers' role in the security arena. While some people do indeed want and value advice, we cannot assume this openness, nor that people should necessarily accept our suggestions or assistance. The human need for autonomy has to be respected [19].

II. Study 1: Offering Memorial Assistance

We carried out an online study that offered participants a new way of memorising their PINs to see whether it improved retention. We decided on an online study to facilitate repeated returns at increasing intervals, something difficult to achieve in the lab.

A. Memorial Aids

We first reviewed the literature to identify candidate memorisation strategies. One very powerful technique is mnemonics [3], where you try to make a sentence from the PIN. The power of mnemonics is observed even in older adults who usually find memorisation challenging [8]. Jakobsson and Liu [14] proposed deliberately generating PINs that create a meaningful mnemonic when typed in. Their scheme was moderately successful but ≈10% of their participants failed to understand how to enter their PIN. This mechanism was unsuitable for our online study since the potential for misunderstanding would be even greater than in Jakobsson and Liu's study.

Repetition reliably helps people to remember new information [18]. With respect to PIN memorisation, such repetition could be either active (person engages in some activity with the PIN pad) or passive (person watches animation of PIN being entered into the PIN pad). There is evidence of the efficacy of both of these approaches, but not specifically in the PIN context.

Visualisations also seem to be particularly promising in supporting PIN memory, since De Luca *et al.* [7] found that participants in their study remembered their PINs as a shape – essentially a visual artifact. We settled on two ways of combining repetition:

1) Repeated PIN entry animation: combining passive repetition and visual memory: Once the PIN is issued, the PIN entry process is animated on the PIN pad three times, each one initiated by the participant. Passive participation is provided by the animation, and the entry shape is visualised.

2) Active repetition of PIN entry: combining active repetition and visual memory: Once the PIN is issued, this technique requires the PIN to be entered three times via the PIN pad. Active participation is assured, and the entry shape is visualised.

B. Fixing PIN length

PIN length varies from 4 to 6 digits globally. To decide on PIN length for this study we ran a survey on CrowdFlower and elicited responses from 400 people. 314 (79%) of the respondents had 4-digit PINs, and almost a third of these experienced difficulties remembering their PINs. A 4-digit PIN is the length people remember best [13], probably because it chunks so well [6]. We did not want to pose an unrealistic memory task so we used 4 digit PINs for the study.

C. Study Design

We formulated the following hypothesis:

H_1: *The memory aids will lead to improved PIN retention.*

We carried out a between-subjects online study to test the hypothesis. Participants were randomly assigned to one of three groups: *control, repeated PIN entry animation* and *active repetition of PIN entry*.

Our participants enrolled and were then invited by email to return at set intervals to re-enter the PIN. Note, we used the time intervals from the well-established forgetting curve [9] because it helped us to identify meaningful intervals to support comparison. During enrolment, the following steps were involved: (1) Provide instructions and collect demographics; (2) Issue a random PIN. Experimental groups then engaged in a repetition exercise; (3) Enter the PIN from memory. If they failed, they were offered another two opportunities.

At return (four times), participants were asked to re-enter their PIN. If they failed, they were offered another two opportunities. During the first and last return rounds we posed some questions. We asked them to tell us what strategies they deployed to remember their real-life PINs and which one they used for the study PIN.

Recruitment and Sample. Our goal was to recruit a broad range of people with diverse backgrounds and age ranges. We asked our friends to forward the study link to their friends and family and to post it on Facebook, using a snowballing technique [12]. Participants were motivated by a lottery draw of a €40 Amazon voucher. 179 participants took part; 93 completed all 5 phases (29, 32, 32 per group, respectively); the majority were between 18 and 39 years of age.

D. Results

1) PIN Retention: There was no significant difference between the three groups so we rejected H_1.

2) Pre-Existing Memorial Strategies: We analysed participants' free text responses to the question '*How do you usually remember PINs?*'. The authors independently reviewed a subset of answers and identified codes (i.e. sub strategies) and categories (i.e. strategies) from participants' responses. These were discussed and agreed upon, resulting in the following eight strategies (in order of prevalence):

- *Visualise:* (pattern/path/movement on the PIN pad);
- *Associate:* (e.g. linking to some number they already know: dates, postal, house or telephone numbers, arithmetic, stories;
- *Split up:* (e.g. by learning a pair of two-digit numbers instead of four);
- *Learn by heart:* (e.g. by saying it aloud);
- *Sounds of buttons*;
- *Repeat:* with or without specifying how (referring to one of the first strategies);
- *Record:* not memorising but rather recording it on paper or on the smartphone;
- *Nothing special:* including statements such as 'just remembering'. The few that did not match any of these eight strategies were assigned to 'others'.

Some used the same strategy regardless of the PIN digits, some varied their strategy depending on the PIN digits, some were willing to accept advice/assistance whereas some preferred to stick to their usual ways of doing things. Finally, some preferred to record their PINs and did not even attempt to memorise them. The free text responses showed that just over half of the participants said they had used the experimental aids (35) to memorise the issued PIN.

E. Discussion

A few explanations for the poor performance of our memory aids suggest themselves. The first explanation could be that the mechanisms themselves were unhelpful. We do not have evidence to conclude this because half of the participants said they did not use them. Since we promised our participants their anonymity we cannot link those who did not use the aids to their actual performance, and we could not remove the detractors. Many of the participants told us which strategies they usually made use of to memorise PINs, and our analysis suggested that they used the same one for the experiment PIN. Since favouring familiar strategies is a human propensity in other areas [17], this is plausible for PINs too.

There is also a second possibility: that they did not take the experiment seriously. This is always a risk with online studies. The only evidence we have that they are likely to have taken it seriously is that they returned to re-enter their PINs four times, and answered our survey questions. This suggests a measure of commitment to the process.

The only thing we could conclude, reliably, is that the bigger issue of PIN management, and intervention by offering memorial assistance, deserved greater scrutiny. A greater understanding of mental models will help us to offer advice to those who do want our advice.

We gained an initial insight in these mental models from our first study:

- *Popular Strategies:* A sample of all the possible memorisation strategies were gathered.
- *Openness to taking advice:* People differ in terms of their openness to considering and adopting new strategies.
- *Use of PIN dependent strategies:* Some people use one strategy for all PINs while others use PIN-dependent strategies. This seems understandable since some PINs produce easy patterns on the PIN pad (e.g. 9852 to the letter 'L') and others can be easily associated to a date (e.g.1231 for New Years Eve) or to a story (4511 - holding a cloverleaf (4) in my hand (5 fingers) on my way to a soccer match (11 players)).

III. Study 2: Mental Models underlying PIN Management

To derive a comprehensive mental model, it is necessary to explore all three options depicted in Fig 1. We conducted three independent studies in order to avoid framing effects. Since recording is generally advised against we felt that we should not mention memorisation in the same survey because it might not elicit a genuine response. Since we were separating out PIN recording, and since PIN changing is also ill-advised, we separated out the survey into PIN changing motivations, too.

Analyses. Free-text responses in all surveys were analysed in a similar way to the free-text responses in Study 1.

Recruitment. Our goal was to recruit a broad range of participants with diverse backgrounds and age ranges. We advertised each survey independently on CrowdFlower in order to achieve this.

A. Memorising the PIN

1) Study Design: We already gained an initial idea of the range of memorisation strategies deployed by PIN holders. The goal of the second study was to augment the initial list. We designed an online survey comprising two stages.

First, we asked respondents to tell us which strategies they would use to remember seven different provided PINs. We selected PINs that lent themselves to usage of the two most popular strategies (visualisation and association) mentioned during our memorial study:

- 1458 – tetris shape when *visualised*
- 9852 – letter 'L' when *visualised*
- 2412 – Christmas Eve when *associated with a date* or $24/2 = 12$ when *associated with arithmetic* or triangle when *visualised*
- 1109 – Sept 11 when *associated with a date*
- 6463 – $63 = 64 - 1$ when *associated with arithmetic*.

We included 9402 and 1603 too because no obvious technique suggested itself. Both lend themselves to a story, to simplification by splitting, or to association with a date (February 1994 and the 16th of March).

Second, we provided respondents with a list of memorisation strategies derived from the previous study. To see whether they would be willing to change the strategy they chose originally, we asked them to re-think the strategies they had previously nominated for each PIN. We asked them to change their previous strategy if they wanted to.

2) Results: 202 people participated in this survey.

Memorial Strategies. No new strategies emerged but a number of new sub-strategies for the strategy *associate* were identified, namely:

- *Letters on PIN pad*, e.g. for 6463 they could remember MIND or MINE.
- *Dates of all kinds*, e.g. moved house, deaths.
- *Times*, e.g. the time of a TV program.
- *Ages*, e.g. two ages (54 and 48 being the ages of their parents).
- *Other kinds of numbers*, e.g. vehicle numbers, numbers in movies;
- *Homonyms*, i.e. associate numbers with words that sound similar.

Openness to change. 49 participants (of 202) changed at least one strategy after having seen the list of strategies. Only one subject changed the deployed memorisation strategy for all the PINs.

PIN-Dependent or Universal Strategies? 43 respondents used the same strategy for all seven PINs (e.g. all visualisation-related memory, only dates, only arithmetic calculations). 157 applied different strategies for the different PINs (from two to six different strategies).

Further insights. Participants used a range of strategies for the same PINs. For example, for the PIN 1109, 54 of the respondents associated it with September 11, the date of the 911 disaster. The next most popular option was visualisation, used by 27 respondents. Visualisation was also used for 9402 and 1603 although these PINs do not produce a particularly easy pattern on the PIN pad.

B. PIN Recording

1) Study Design: We designed an online survey to explore PIN recording behaviours. We asked whether the participants' bank advised them against recording their PINs, and whether they had recorded a PIN (in any way). We asked them to explain their motivation either for recording, or not. We also asked them to tell us how they recorded their PINs, if they did so.

2) Results: We elicited 200 responses. 107 recorded their PINs (75 of them knew they should not), 82 did not record and 11 could not remember whether they had done so. 141 said their bank advised against recording their PINs. An analysis of the open text responses we revealed the following:

Why respondents recorded PINs. Participants mentioned as motivation that they were concerned about forgetting the PIN and that they worry about the consequences because previous forgetting had led to difficulties.

Recording Mechanism. Some respondents recorded their PINs and take the record with them. Others kept the recorded PIN somewhere safe, as a form of insurance. Many wrote down their PINs on paper or stored them on their mobile phones. Others stored them in a notebook or on their PCs. Two meta recording approaches emerged: insecure (write it down) or secure (use a password manager or apply an algorithm before recording).

Why Respondents did not record PINs. Reasons cited for not recording are that they could remember the PIN, mostly because the PIN was termed 'easy', that it was not good practice to record PINs, and a number simply said: "safety" or "security".

C. Changing the PIN

1) Study Design: We designed an online survey to explore PIN changing behaviours. We asked whether respondents were allowed to change their PINS, and, if so, whether they had done so. Whatever their response, we asked them to explain why they either had, or had not, changed their PINs.

2) Results: We elicited 200 responses. 149 were permitted to change their PINs and 103 had done so.

Why Respondents changed PINs. The following themes emerged: many said simply: "safety" or "security". Some spoke about the need to make the PIN more memorable, the need to change after having lent the card and PIN to someone, or that their bank issued a default PIN and there was an expectation that this would be changed.

Why Respondents did not change PINs. The identified themes here were that they felt safer with the issued (random) PIN, that they did not see a strong need to change the PIN. The reasons for this included the PIN being 'OK', because they could easily remember it, because they did not feel like it, or because it was too cumbersome to change the PIN.

IV. Discussion and Mental Models for PIN Management Strategies

We derived the model depicted in Fig 3 that encapsulates the different mental models.

A. Openness to Change

The participants in our studies, when the questions elicited a relevant response, seemed to fall naturally into two groups: those who were open to advice and those who were content with their *status quo* practice. It is important for researchers to acknowledge this. Humans have a psychological need for autonomy [19], that is, the right to make their own decisions. Furthermore, people seeking to give assistance in any area, where it is not wanted, may well be considered to be "butting in" [11]. There is a personal cost to taking advice that this group might have been unwilling to pay, even in an anonymous online study. Humans also have a need for competence [5]. Since the respondents have been managing their own PINs for years they might have been unwilling to admit any deficiency in this area [15]. Both advice takers and advice rejectors must have taken part in all our studies and they certainly made their presence felt in Study 1.

In conclusion, banks should indeed offer advice for PIN management, but we need to respect people enough to acknowledge that they might not want or need advice. Advice should be available but not pushed onto people who do not want it.

B. Memorizing the PIN

Some people have one strategy, and use it for all their PINs. Most, however, use PIN-dependent strategies. Two were dominant: **visualisation** and **association**. Association is a rich category with many sub-categories. People, especially new PIN holders, might well be unaware of the range of sub-strategies so they might benefit from being made aware of them.

As the primary motivation for changing or recording is to ensure memorability, it is possible that the prevalence of these insecure practices could be reduced by making people aware of the full range of association sub-strategies.

C. Coping Strategies

It is clear from our reported results that people engage in a variety of coping strategies with respect to PIN management. They record PINs despite prohibition from banks, and many change their PINs, probably to more predictable or weaker alternatives.

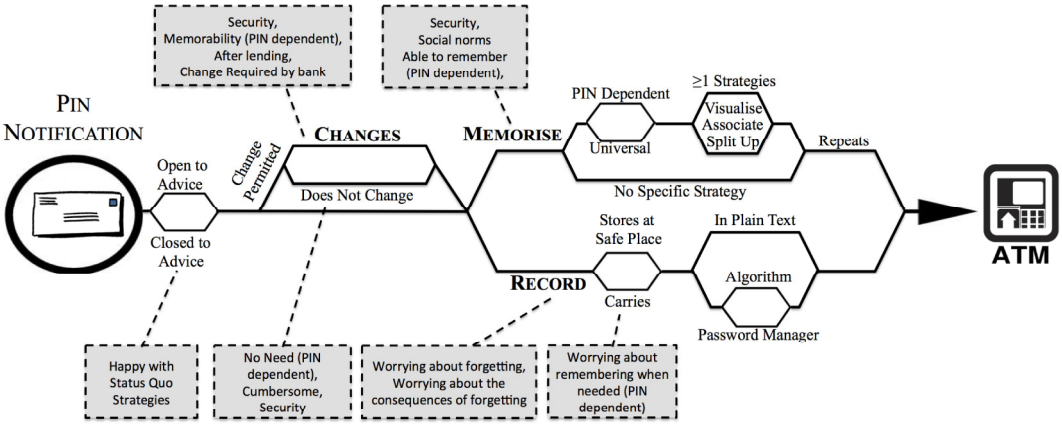

Fig. 3. Mental Models for PIN Management Strategies based on findings from Study 1 and Study 2. It includes the set of possible decisions and possible reasons where available.

1) Changing the PIN: Some people changed their PIN for security reasons. Respondents did not qualify this by saying that it should be changed if leaked, only that it should be changed regularly. While changing is wise if the PIN has been divulged, doing so to protect against the bank potentially knowing the PIN is a misperception. Regular password changes are advised, and people might change their PINs because they conflate passwords and PINs in their minds. In reality PINs cannot be leaked by people sniffing the network, but they can indeed be leaked by people observing them being entered in multiple locations as people use them in their day-to-day lives. Both eventualities should be addressed when offering advice.

2) Recording the PIN: It is necessary to accept and support people's need to record their PINs. When one attempts to forbid something that people are determined to do no one wins (The lessons learnt from the American Prohibition period are instructive here [2]). Recording might be a particularly sensible option for elderly people whose adult children have to manage their finances for them. It is probably time for banks to acknowledge this reality with an aging global population with memory difficulties. In general, it is far better to acknowledge that the behaviour exists, and to try to direct it to a more secure path.

V. Kinds of Advice

The relevant advice sections from a PIN notification letter received by one of the authors from a UK bank advises immediate memorising, and offers the opportunity to change. It forbids PIN recording.

Based on the findings from the previous sections, we propose that more realistic and nuanced advice should be offered, as well as addressing and acknowledging the prevalence of all three PIN management strategies. We will now consider what kinds of advice should be offered.

A. Memorisation Advice

From our findings, we derived the following recommendations:

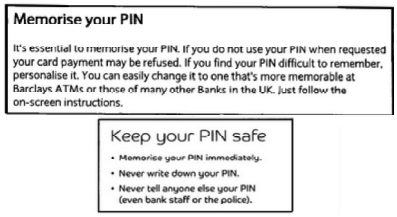

Fig. 4. Excerpt from the Bank PIN Issue Letter.

- Start off by explaining that different strategies might suit different PINs.
- Advise repetition – while learning but also during the first couple of days.
- Provide a PIN pad to ease visualisation of the path for the issued PIN.
- Explain that using the letters might help but that some PIN pads do not contain letters. (They can choose to patronise only the ones that do)
- Provide an example for each of the most popular strategies.

B. Secure Recording Advice

Similar to Bonneau *et al.* [4], our participants admitted recording their PINs, despite prohibition from the banks. We therefore recommend:

- Introduce secure recording with password managers.
- Explain how to 'encrypt' the PIN by applying an algorithm (e.g. adding or subtracting 1111 before recording).

C. Secure Changing Advice

We recommend explaining why and when PINs should be changed. To mitigate against poor PIN choices, we recommend offering a list of the most predictable PINs to avoid.

D. How to Present the Advice in a Leaflet

The leaflet should clearly indicate that it is in the nature of a friendly suggestion, and does not mandate compliance

(i.e. tactfully offering advice). For those who are prepared to accept the advice, we recommend providing a procedure to go through for the issued PIN starting off with memorisation as the advised option, then securely changing followed by securely recording.

VI. Ethics and Limitations

Ethical requirements for research involving human participants are provided by an ethics commission at the University. Relevant ethical requirements regarding participant consent and data privacy were met. Participants were instructed not to provide any of their own PINs in their responses.

Limitations: When you survey people about anything security related, like PINs, anonymity becomes essential. By using CrowdFlower for our follow-up surveys in Study 2, we hoped that the anonymity it afforded would give people enough reassurance to encourage honesty.

Our follow-up surveys relied on self-report. Thus, we actually cannot guarantee that respondents were truthful. We do not see any motivation for them to disseminate so we do not believe this to be a serious threat to the validity of our research.

VII. Related Work

A number of researchers have proposed assistance to help people with their PINs. For example, Renaud and Smith [16] proposed a mechanism called 'Jiminy' for secure recording of 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 (see Fig 5). Spydeberg Sparebank came up with an alternative mechanism which assists customers by providing a credit-card sized cutout (see Fig 5). 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 [1].

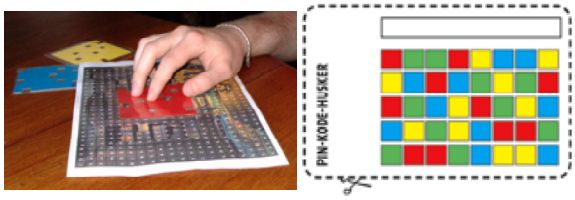

Fig. 5. Jiminy approach as proposed in [16] (left) Spydeberg Sparebank Memory Card (*circa* 2005) (right)

The failure of these two mechanisms, as well as the ones we trialled, could well be because we did not understand extant PIN management mental models, and the motivations for PIN management strategy choices. Now that we have a better insight, we propose providing a leaflet for issue with new PINs, rather than a single new memorial or storage mechanism.

VIII. Conclusion

The original motivation for this research was to find out whether we could help people to memorise their PINs, indirectly encouraging them to behave more securely. We tested two visual repetition-based memorial strategies but found that they did not improve PIN retention and that many of the participants did not make use of them. Instead some preferred to stick with their tried and trusted strategies for managing PINs. Our study highlighted the need to respect the autonomy of our users when offering advice.

References

[1] 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.

[2] E Behr. *Prohibition: Thirteen years that changed America*. Arcade Publishing, 1996.

[3] F S Bellezza, L S Six, and D S Phillips. A mnemonic for remembering long strings of digits. *Bulletin of the Psychonomic Society*, 30(4):271–274, 1992.

[4] 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.

[5] James P Connell. Context, self, and action: A motivational analysis of self-system processes across the life span. *The self in transition: Infancy to childhood*, pages 61–97, 1990.

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

[7] A De Luca, R Weiss, and H Hussmann. Passshape: stroke based shape passwords. In *Proceedings of the 19th Australasian Conference on Computer-Human interaction: Entertaining User interfaces*, pages 239–240. ACM, 2007.

[8] A Derwinger, A Stigsdotter Neely, M Persson, R D Hill, and L Bäckman. Remembering numbers in old age: Mnemonic training versus self-generated strategy training. *Aging, Neuropsychology, and Cognition*, 10(3):202–214, 2003.

[9] H. Ebbinghaus. *Über das Geddachtnis: Untersuchungen zur experimentellen Psychologie*. Duncker und Humblot, Leipzig, 1885.

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

[11] D J Goldsmith and K Fitch. The normative context of advice as social support. *Human communication research*, 23(4):454–476, 1997.

[12] L A Goodman. Snowball sampling. *The annals of mathematical statistics*, pages 148–170, 1961.

[13] J H Huh, M Bashir, H Kim, K Beznosov, and R B Bobba. On the memorability of system-generated PINs: Can chunking help? In *SOUPS*, Menlo Park, California, 9-11 July 2014. http://cups.cs.cmu.edu/soups/2014/workshops/papers/chunking_huh_11.pdf.

[14] M Jakobsson and D Liu. Bootstrapping mobile PINs using passwords, 2011. http://www.markus-jakobsson.com/wp-content/uploads/W2SP11-JL.pdf (Access Date: 6 August 2015).

[15] F Lee. When the going gets tough, do the tough ask for help? help seeking and power motivation in organizations. *Organizational behavior and human decision processes*, 72(3):336–363, 1997.

[16] 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.

[17] G Salkeld, M Ryan, and L Short. The veil of experience: do consumers prefer what they know best? *Health economics*, 9(3):267–270, 2000.

[18] A A Smirnov. The process of repetition. In *Problems of the Psychology of Memory*, pages 245–259. Springer, 1973.

[19] S S Wichmann. Self-determination theory: The importance of autonomy to well-being across cultures. *The Journal of Humanistic Counseling*, 50(1):16–26, 2011.

