8

Mental Models of Password Managers

An important spillover of our previous exploration is that password managers are more likely adopted the longer people had struggled with juggling passwords: Older participants in the third personality study were more likely to use a password manager (PWM). We have already corroborated market surveys that indicate a generally low adoption rate of password management software. As discussed in Sections 3.2 and 3.3.4, it has been hypothesized that users do not fully trust third parties with their credentials, so there seems to be an urge to stay in charge. Consequently, most users still try to memorize their passwords. On the other hand, password managers do provide many usability and security benefits, but why do users fail to see them? To this end, we see a lack of understanding about how users make sense of password managers. Our goal was to understand users' mental models of password managers first and then identify opportunities to improve them, which could increase adoption rates. We thus aimed to answer the following research questions: **(1)** How do users think a password manager works? **(2)** How does adopting a password manager change user attitudes and behaviors?

To answer these questions, Martin Prinz and I explored attitudes and understandings in semi-structured qualitative user interviews. To get a more complete picture, we interviewed both people who already use a PWM and also people who prefer other coping strategies. Parts of the outcome of this investigation have been published as an extended abstract at SOUPS 2017 [248].

8.1 Background and Context

Password managers can be either built into web browsers or act as a standalone solution that is independent of the password's purpose. Dedicated password managers have existed since the mid to late 1990s. Web Confidential[1] was probably one of the first programs to facilitate password management, when it first surfaced in 1998. However, which of the browsers was first to add password storage capabilities cannot be easily traced back, but all major browsers added this feature in the early 2000s. Given the long history of supporting authentication with software tools, adoption of password

[1] http://www.web-confidential.com/ *(last accessed 16.02.2018)*

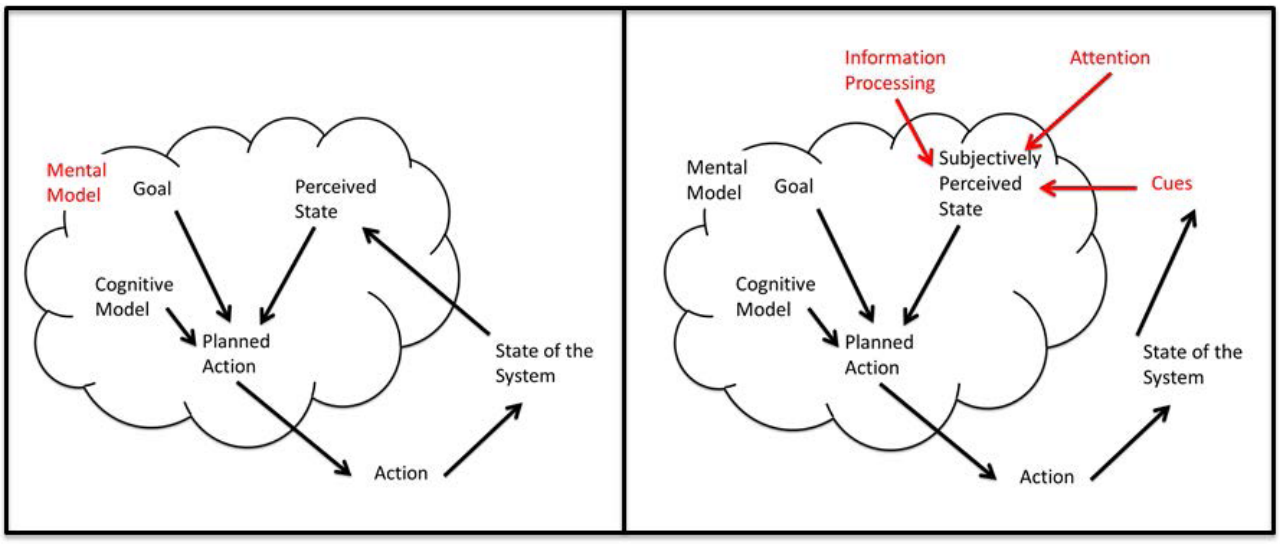

Figure 8.1: Volkamer and Renaud see the formation of mental models as loop involving different plans, perceptions, system structures, and actions. Image from [337]

managers is still at only 12% [239]. Even security experts disagree on the specific security benefits of different implementations[2]. If the auto-fill feature is enabled, this can be used to create digital footprints for individuals[3]. Nevertheless, similar attack vectors could easily target regular password entry, and are not limited to auto-fill.

There are different service architectures for handling passwords: *offline* password managers keep a database of encrypted passwords locally on the user's machine, while *online* managers provide more mobility because passwords are held on a server or a distributed storage solution [223]. *KeePass* and *Password Safe* are notable representatives for the offline storage paradigm, while the cloud-based approach is dominated by third-party solutions like *LastPass*, *1Password*, and *Dashlane*. Browser vendors have also transitioned to store passwords in the cloud, e.g. Apple Keychain for Safari, or Google Smartlock for Chrome. On the one hand, this provides consistent user experiences across multiple devices. On the other hand, such architectures create lock-in effects and dependencies. Thus, online password managers typically provide browser-extensions to automatically fill username and password fields. This way, similar experiences are achievable by third party tools.

Mental Models Norman suggests that exploring mental models provides predictive and explanatory power for understanding an interaction [237]. Volkamer and Renaud meticulously described different aspects and definitions of mental models, which are too elaborate to discuss in this work [337]. As a takeaway, a mental model describes a user's sense-making of any system they interact with. Volkamer and Renaud highlight that mental models are not necessarily static, but can be shaped with different cues to internal feedback loops (see Figure 8.1). For our purposes, we use a simpler definition provided by Young: Mental models are "collections of the root reasons why a person is doing something" and "represent what a person is trying to accomplish in larger context, no matter which tools are used" [369, p.11]. In our case, they describe the reasons for (not) using a password manager, as explained by current actions to cope with authentication tasks.

In chapter 5, we took a quantitative approach to elicit data on the mental models. This was useful

[2] https://www.wired.com/2015/07/websites-please-stop-blocking-password-managers-2015/ *(last accessed 16.02.2018)*

[3] https://freedom-to-tinker.com/2017/12/27/no-boundaries-for-user-identities-web-trackers-exploit-browser-login-managers/ *(last accessed 16.02.2018)*

because we tried to understand *what* contributed to password strength perceptions and by *how much*. For password managers, related work on usage motivation is scarce, thus we strove to answer *why* users perform certain actions and *how* these could be supported by a password manager. Therefore, qualitative methods were more useful. Eliciting such data to understand mental models, Bravo-Lillo et al. relied on open-ended one-on-one interviews both with advanced and novice user groups [38]. They highlight the usefulness of this approach to understand thought processes. Kang et al. relied on *drawing tasks* to elicit additional data [183]. Participants were asked to sketch what they thought happens to their personal data when they interact with different online services. During sketching, a *concurrent think-aloud protocol* was used to avoid misunderstandings. Once the data has been collected, Young suggests the *affinity diagramming* method to derive themes and identify opportunities for supporting tasks [369]. In this research project, we combined interviewing, drawing tasks, and affinity diagramming.

8.2 User Interviews

Our main objective was to understand how users make sense of password support tools, in particular password managers. This would allow us to explore solutions that fit user expectations better.

8.2.1 Method and Protocol

Focusing on attitudes and mental models requires a qualitative study method. We chose to conduct semi-structured, open-ended interviews. The sessions started with a thorough briefing about the study purpose and asking for permission to audio-record the conversation. The main questions were **(1)** *Why do you need passwords?* and **(2)** *What is your strategy to manage multiple accounts?*. From there, the study followed a more fine-grained follow-up questions to investigate the specifics of these two aspects. Moreover, Bravo-Lillo et al. showed the benefits of drawing tasks to find structural patterns in beliefs [38], so we also asked participants to **(3)** *sketch how a password manager works*. This required that participants were aware of PWMs. If they were not, they were told that it is a "piece of software that stores a user's password", which was expected to be vague enough to explore participants' expectations of this kind of software. The interviews took between five and 16 minutes.

Recruitment and Sample

We first approached random passers-by on a popular street in Munich to obtain a diverse sample of participants. Six interviewees were recruited this way. However, these first six interviews showed that participants were unable to provide sufficient detail in answers to allow thorough analysis. Thus, we changed the recruiting method and approached employees of a design agency with which we had collaborated in the past. We also knew that the agency's policy required employees to utilize password managers. Moreover, the user group was more likely capable of visually expressing mental constructs, allowing for the envisioned analyses. Eight additional participants were interviewed in this sample, giving a total of N=14. They worked as experience designers and concept developers, and did not have formal training in computer science or engineering. The age of all interviewees ranged from 20 to 41. **@TODO** listen to recordings and determine gender distribution (CD in Munich).

None of the interviewees in the first group had used a password manager before, so we call this participant group the *novices*. Since the PWM was part of the company policy, all interviewees in the second group had used one before, so we call them the *actives*. The separation allowed us to detect a

shift of expectations before and after adopting a password manager.

Method Limitations

The recruiting and sampling methods are inherently limited. The novice user group was asked at a public spot, so it was difficult to provide enough context information and minimize distraction. On the plus side, we achieved diversity and the face-to-face set-up reassures trust, because it was clear that none of the information they gave us was going to be used to access their online accounts. 5 of 6 *novices* were unable to describe what a password manager was, before we gave them the above definition. Thus, their decision to refrain from using a PWM was not made actively, but rather results from the lack of awareness. This limits the analysis of attitudes and self-reported behavior. Finally, the second user group has a homogeneous background: design and communication. All these limitations demand that the results not be generalized to a larger population. Instead, they should be seen as rough trends that help understand a first set of underlying mental models, rather than the entire spectrum thereof.

8.2.2 Data Analysis and Results

Young proposed a design strategy to translate qualitative data into mental models [369]. The method is based on *affinity diagramming*. The resulting clusters and themes from the diagram are then mapped to a hierarchical structure that consists of Mental Spaces, Task Towers, Tasks, and Particular Tasks. Here, we focused on those Mental Spaces and Task Towers that involve password managers. Table 8.1 shows the resulting model in this format. In the following, we report the results that notably contributed to the formation of the model, which is described in Section 8.3.

Selection and Coping Strategies

All interviewees reuse passwords to cope with the multitude of accounts. Participants often developed coping strategies without deliberation: they were unaware of how they cope with passwords until we specifically requested more details. Only then did they reflect and realize how they behave. One such revelation was that they categorize passwords in different ways. For instance, the context in which they created an account, e.g. the URL or policy of the corresponding website, was factored into passwords and facilitated the decision-making process which password to choose from their portfolio (see Figure 8.2 A). Similarly, the perceived importance led to distinct categories, although the interviewees had not realized this. Furthermore, we also heard an interesting, deliberate strategy that seldom appears in the literature: two participants mentioned memorizing a list, or a list of letters that are then transformed into a new, quasi-unique password. This method is comparable to the Diceware technique (see 3.3.3), but instead of rolling a dice, these participants algorithmically select the order of words/letters based on contextual cues (see Figure 8.2 B and C). Another participant said to have memorized a randomly generated password and reusing it many times. Finally, participants generally tried to justify their "insecure" behavior. Beside memory burden of new secrets, time pressure was mentioned as reason for password reuse.

We also inquired situations when their strategies failed. The primary problem of having a multitude of accounts was the correct *combination* of user-name and password, which is a common pitfall of knowledge-based authentication [303]. Not only did they forget passwords, but also user names, which is just as severe because web sites generally do not inform users which was the error source to thwart attacks. Participants reportedly use a trial-and-error to go through their portfolio and ultimately use self-serviced password resets as a convenient solution. Interviewees expected that websites offer this kind of fallback scheme, because two of them do this on a regular basis.

Mental Space	Task Tower	Tasks
Creation & Selection	Influential Factors	Personal & Historical
		Policies & Rules
		Algorithmic Strategies
		Account Context
		Memorization
	Support Tools	Generate & Memorize
		Use given Password
		Generate & Digitally Store
	Personal Algorithms	Passphrases
		Reuse Word Blocks
		Base-Password with Modifications
		Website Influence
		Use Reduced Alphabet
	Handle Failures	Trial and Error
		Lookup Password
		Show Entered Password in Plain Text
		Reset Password
Log-In	Manual Tasks	Copy & Paste password
		Lookup hints and cues
		Recall from memory
	Simplify	Stay logged-in
		Cross-device support
		Autofill forms
		Rely on manager
Organize and Commit	Share Passwords	Secure sharing with colleagues or friends
		Write down password
		Reset after sharing
	Use Aid	Password Manager
		Word/Digital Document
		Handwritten Notes
	Memorize Passwords	Algorithmic
		Website Cues
		Mental Drawer
		Base Password and Modifications
	Protect Passwords	Modify Passwords
		Unlock access with Master Password
		Hide or Encrypt File/Notes
	Automation	Reset Multiple Passwords
		Autosave Credentials
		Autofill Username and Password
		Warnings when websites are compromised
	Build Password Categories	Security
		Importance
		Frequency
		Policies & Rules
		Mental Drawer

Table 8.1: Mental Model of Authentication and Password Management, adapted from Martin Prinz [247]

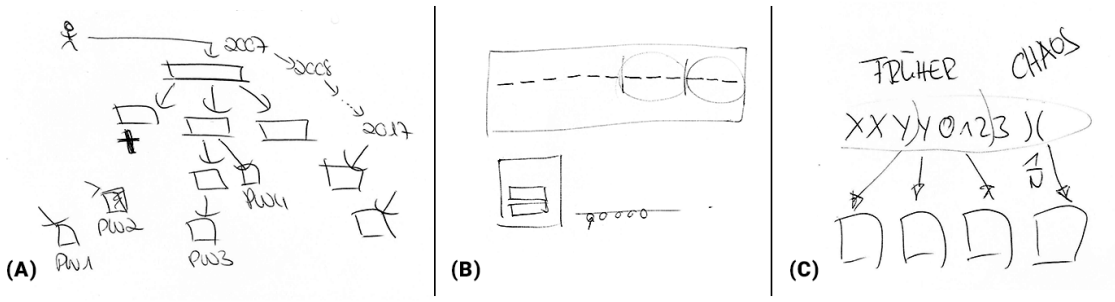

Figure 8.2: Participants were asked to visualize their methods to create passwords, if they had a specific strategy. (A) participant who categorizes and remembers passwords by the time they were created (context factors). (B) participant uses words and cued positions to recall the constellation. (C) participant who uses a fixed set of characters and algorithm to "calculate" the correct constellation.

Password Manager Impact

Overall, the *novices* and *actives* did not behave differently in their selection and coping strategies at first sight. However, we found that *actives* did in fact change some habits when they had started using a password manager. First, although they were initially exposed to PWMs at work, *actives* started using them in private shortly afterwards. This interaction and experience with the tool led to their migrating passwords into the manager step by step. One participant mentioned that it helps him stay organized where there was "chaos" before (see Figure 8.2 C). Others were somewhat ashamed of their weak practices before using this kind of software. Password sharing with other users was the central advantage for four interviewees, especially at work. It facilitates secure collaboration with colleagues and clients. Participants do not memorize these passwords, because they often use built-in password generators. They realized that shared passwords are short-lived because colleagues leave or contracts with clients end, upon which passwords are invalidated. One interviewee fully embraced generated passwords even for private purposes and only memorizes his master password. Interestingly, however, for their most important accounts, most *actives* kept on manually crafting passwords and refrained from putting them into the PWM. Having used the tool and become aware of their own weak behavior in the past, they had gained confidence in selecting stronger passwords. This gain of mastery left them with a positive experience of password managers. As a contrast, *novices* were all comfortable with how they managed their passwords and did not show that sense of insecurity.

Drawing Tasks

Participants were asked to sketch their thoughts whenever this was appropriate. We encouraged them to sketch as much as possible. All participants mentioned that it was challenging to communicate their understanding this way. Already for basic functionality and purpose of passwords, we asked to create sketches. This task was still relatively easy for all interviewees. Padlocks and keys were two of the most commonly drawn elements. It also helped to communicate individual elaborate selection strategies (see Figure 8.2). However, the difficulty rapidly changed for the workings of a password manager. Here, especially *novices* struggled with the task and could not proceed without further explanation, and their drawings were more vague than those of *actives*. However, the latter is probably due to the different professional background and expertise in creating concepts. The drawn elements and metaphors differed among the two groups:

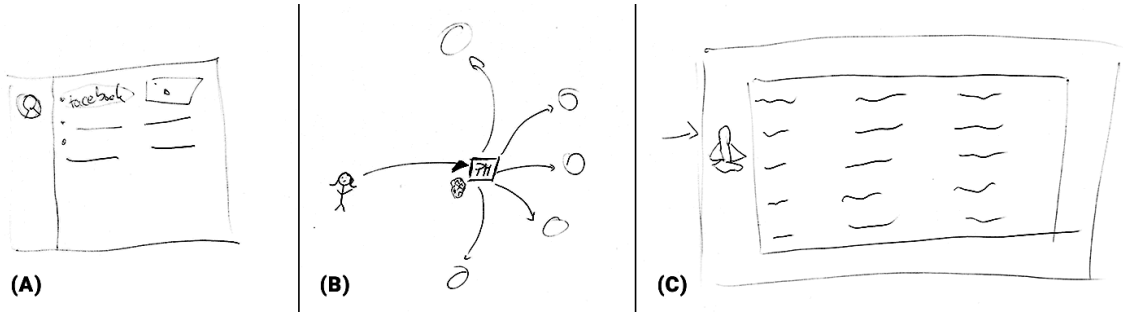

Figure 8.3: Drawings to the question "What does a password manager do, and how?" from three *novice* users. (A) only shows a profile on facebook. (B) emphasizes that the PWM is a central hub and acts as the user's "brain" for different entities. (C) shows a table-like structure that holds all username-password tuples.

Novices had a vague model of how such a password manager might work and found it especially difficult to sketch this. The benefits and system architecture of the software were unclear to them. One interesting drawing depicted a password manager as a virtual "brain" that acts as a central hub to make the user's life easier (Figure 8.3 B). Another participant, who reportedly used a Word document to keep track of his accounts, imagined a password manager to behave the same way (Figure 8.3 C). The only expected difference would be that accessing the list of passwords would be protected by a password, which is indicated by the keyhole and an arrow that points to it. This represents *novices'* understanding on a more general level, as they explained a password manager as a special way to manage a *secure list of passwords* that helps find the right ones. Five said that it facilitates logins by allowing them to **copy-and-paste** passwords from the manager into the webpage.

Actives Since all active users were also visual communicators, it was somewhat easier for them to sketch the workings of a password manager. They clearly focused on the interaction between users and the system and highlighted the benefits in their drawings. Having experienced the advantages, they strove to convey these visually and came up with more details (cf. Figure 8.4). Instead of a password-table, we can see workflows that show the interplay between user, database and website. Common components are UI elements like input fields or buttons that link to other screens or entities. Only one interviewee from the *active* group refrained from UI elements and instead sketched a flow-chart.

8.3 Mental Model

From the behavioral, attitudinal, and experiential data, we created a mental model schema in the style of Young [369]. We tried to stay close to the data as possible, but a few points are enhanced by knowledge from related work. We briefly elaborate on the mental spaces to allow the reader to delve into task-towers and tasks.

Password Creation and Selection First, users have a variety of particular needs when they are challenged to create a password. This task tower describes both the constraints, prior experiences and strategies to accomplish the task. Our participants often mentioned highly individual selection strategies that allow for both secure and memorable secrets. From a support tool, they expected

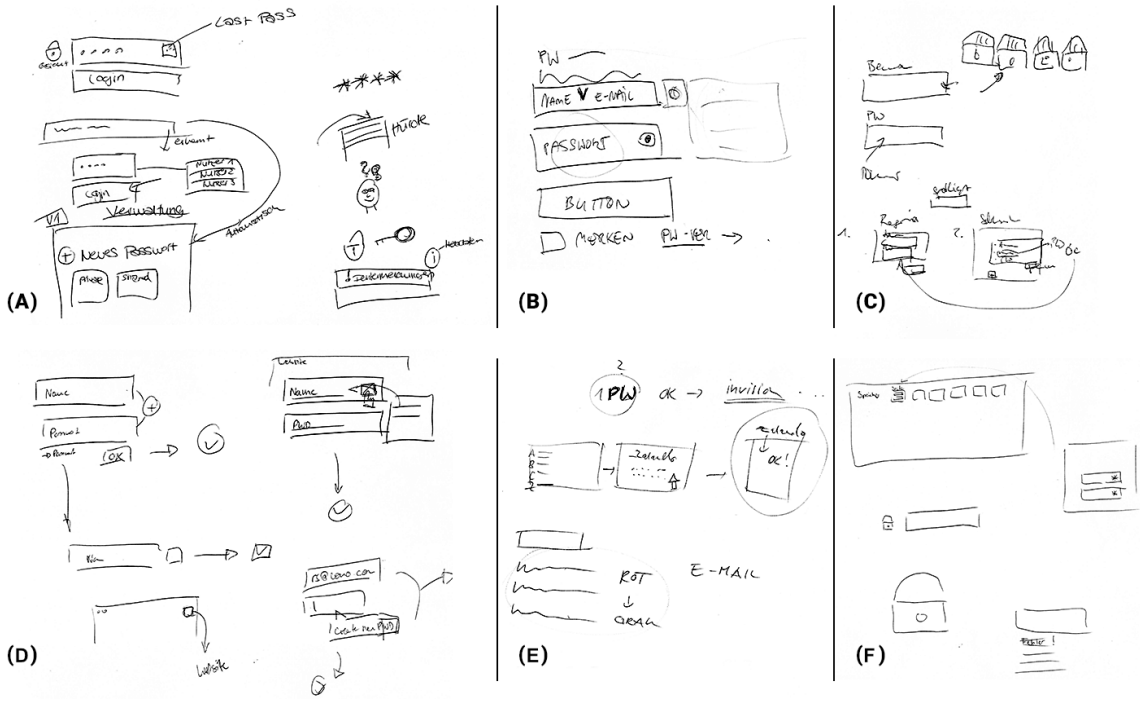

Figure 8.4: Drawings to the question "What does a password manager do, and how?" from six *active* users. Common components are UI elements that link to other entities, therefore the interplay between user, PWM and website is clearer.

guidance and feedback. Password generators that simplify this task can aid here.

Log In Most prominently, authentication still involves *both* manual and automatic tasks. Interviewees expected to copy and paste passwords from the manager to their browser, or at least provide a way to retrieve password hints. On the other hand, participants expected that support tools are deeply integrated into the browser by automatically filling password fields in a highly reliable manner. If possible, the solution should work across multiple devices.

Organize and Commit The third mental space resembles the "Commit to password" and "Live with password" stages of the Password Life Cycle [303]. Each participant mentioned some way of organization strategy that allowed them to live without password managers to some degree. However, these were not always deliberate choices, but rather have formed over the years. Especially *novice* users made sense of password managers by their capability of protecting passwords, i.e. encrypting a list of passwords rather than just storing them in a Word document. *Active* users were already aware of the sharing capabilities and appreciate a simple process to reset passwords when they need to be invalidated for security reasons.

8.4 Opportunities and Challenges

Having fine-grained insights into the mental models of password authentication sub-tasks lets us explore novel ways to support users in many challenges. In the following, we highlight key opportunities for future work on password managers and password support in general.

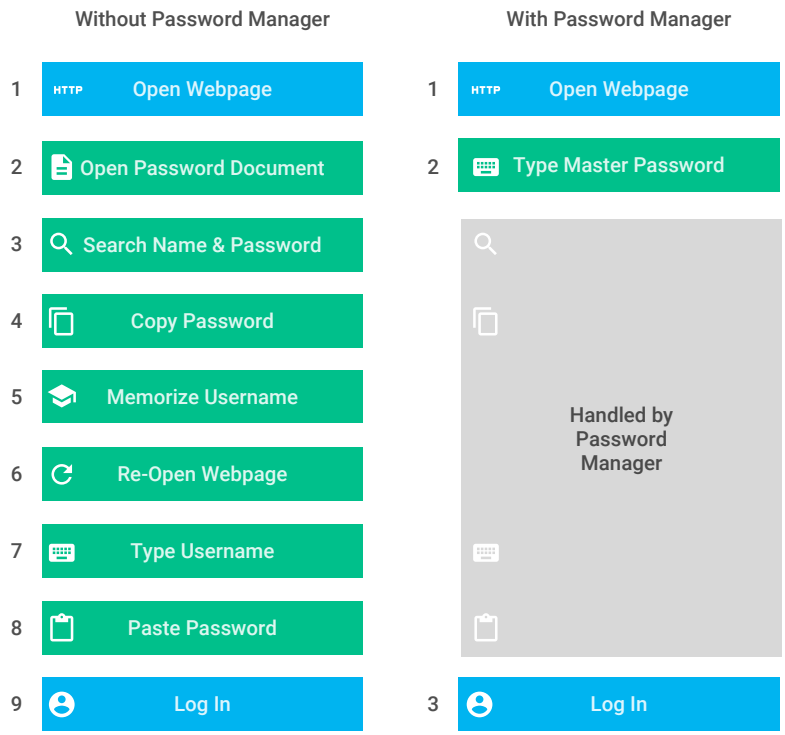

Figure 8.5: Visualizing users' previous behavior might help communicate how the password manager can simplify authentication tasks. This can create a better mental model of their workings.

8.4.1 Leveraging and improving novices' mental models

There were two important preconceptions about password mangers on the *novices* side: simple password lists and copy-paste interactions. Future password managers can leverage these models to persuasively communicate functionality. The value proposition should thus ensure that potential users understand that PWMs are *not only* a secure list of user-names and passwords, but also help them *select* passwords – a benefit that *actives* had realized in retrospect. The *password list* metaphor is also useful to communicate automation features: explicitly showing new users that they do not have to search through the list, nor copy and paste passwords from the list to the website might help them understand the simplicity of the interaction paradigm. This can happen during an onboarding user journey, e.g. with an image showing the steps saved by the PWM (cf. Figure 8.5).

8.4.2 Increasing Sense of Agency

While automation simplifies processes and thus improves usability, staying in control of security-related interactions is important to users. *Novices* were confident in their current behavior. *Actives* had realized that their past behavior was sub-optimal, but they had gained confidence to create passwords and handle authentication for their most important accounts on their own. As a consequence, a password manager needs to stay flexible enough to respect user preferences for different account *categories*, e.g. unimportant vs. important accounts. At the same time, reassuring users that their decision to handle such situations on their own is reasonable and can inspire trust in the system. A PWM could automatically detect when it is appropriate to offer help. Current managers only provide the opportunity to decide whether the password should be saved, maybe saved later, or never be saved for a particular site. Such decisions can be automated once enough training data has been provided by the user.

8.4.3 Leveraging Context

Context factors can be leveraged by PWMs to adapt to different situations. For example, usage-context informs future interactions. If the user sets up the system at work, this is an indicator about how passwords are going to be categorized, how often they will be reset, and how likely they are going to be shared with others. Adapting the interface to such scenarios can simplify interactions and forming mental models of the benefits. Moreover, automated generation of passwords is also context-dependent. As we have shown in chapter 6, password policies in the wild impose varying restrictions on the use of characters. To avoid user frustration arising from rejected passwords, e.g. because they contain forbidden characters, the generator can ensure the random password meets the website's composition policy.

8.4.4 Customization and Personalization

It is evident that current third-party and browser-built-in password managers form a standalone mechanism that works differently compared to how users normally cope with passwords. Our participants reused passwords with different strategies and relied on digital documents, paper notes, and highly individual password creation or memorization techniques. Beside the document-metaphor discussed above, the other strategies are not reproduced by password managers. However, a general philosophy in user-centered design is the aim to "fix the system" rather than to "fix the user". Therefore, the system should provide ways to support current strategies. For instance, it could help the user specify their creation technique: they might use a base-password that is modified depending on the context, the PWM could offer to generate passwords like this in future scenarios. While this approach would not necessarily improve security, it could save the user time and make authentication more usable. Besides, the user stays independent of the tool, because they can reproduce their system and log in on other devices even without the support.

8.5 Conclusion

We explored the mental models of authentication tasks and password managers with a qualitative approach. Both participants experienced with password managers and inexperienced novices shared their insights, attitudes and behaviors during short interviews. Fourteen interviewees provided us detailed descriptions of their password selection and coping strategies, and how they make sense of supporting tools. We contribute evidence that (a) individual coping strategies persist even after adopting a password manager for important accounts, (b) work environments serve as onboarding triggers even for private use, and (c) novices were mostly unaware of the functionality and benefits of password managers. These findings show that the value proposition should be communicated concisely and compare the benefits against inefficient password practices. At the same time, new solutions should respect highly individual coping strategies to better match user behavior. Ultimately, this could increase adoption, and more importantly, retention rates.

Take Aways

- Password managers appear to be a “black box” for people who have never used one. They suspect that such tools are a slightly more secure version of text files to write down lists of username-password-combinations.
- The mental model of password authentication and managers is mostly divided into the mental spaces “Select password”, “Log in”, and “Organize”. There seem to be discrepancies between current user behavior and current password managers.
- Making password managers adapt to context and individuals seems a promising direction for future systems.

Bibliography

[1] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *Comput. Surveys* 50, 3 (2017), 1–41. DOI:http://dx.doi.org/10.1145/3054926

[2] Alessandro Acquisti and Grossklags Jens. 2008. What Can Behavioral Economics Teach Us about Privacy? In *Digital Privacy - Theory, Technologies, and Practices*, Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis, and Sabrina De Capitani di Vimercati (Eds.). Vol. 6545. Auerbach Publications, Boca Raton, FL, USA, 363–374.

[3] Anne Adams and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42, 12 (1999), 41–46. DOI:http://dx.doi.org/10.1145/322796.322806

[4] Anne Adams, Martina Angela Sasse, and Peter Lunt. 1997. Making Passwords Secure and Usable. *People and Computers* 34, 1 (1997), 1–15. DOI:http://dx.doi.org/10.1145/99977.99993

[5] Alexander T. Adams, Jean Costa, Malte F. Jung, and Tanzeem Choudhury. 2015. Mindless Computing : Designing Technologies to Subtly Influence Behavior. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (Ubicomp '15)*. ACM, 719–730. DOI:http://dx.doi.org/10.1145/2750858.2805843

[6] Seb Aebischer, Claudio Dettoni, Graeme Jenkinson, Kat Krol, David Llewellyn-Jones, Toshiyuki Masui, and Frank Stajano. 2017. Pico in the Wild: Replacing Passwords, One Site at a Time. In *Proceedings 2nd European Workshop on Usable Security*. Internet Society, Paris, France, 1–13. DOI:http://dx.doi.org/10.14722/eurousec.2017.23017

[7] Heikki J. Ailisto, Mikko Lindholm, Jani Mantyjarvi, Elena Vildjiounaite, and Satu-Marja Makela. 2005. Identifying people from gait pattern with accelerometers. In *Proceedings of SPIE - The International Society for Optical Engineering*, Anil K. Jain and Nalini K. Ratha (Eds.). Bellingham, WA, 2005, 1–8. DOI:http://dx.doi.org/10.1117/12.603331

[8] Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *Proceedings of the 22nd USENIX Security Symposium*. USENIX Association, Washington, DC, USA, 257–272. http://research.google.com/pubs/archive/41323.pdf

[9] P.S. Aleksic and A.K. Katsaggelos. 2006. Audio-Visual Biometrics. *Proc. IEEE* 94, 11 (nov 2006), 2025–2044. DOI:http://dx.doi.org/10.1109/JPROC.2006.886017

[10] Nouf Aljaffan, Haiyue Yuan, and Shujun Li. 2017. PSV (Password Security Visualizer): From Password Checking to User Education. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Vol. 10292 LNCS. 191–211. DOI:http://dx.doi.org/10.1007/978-3-319-58460-7_13

[11] Patricia Arias-Cabarcos, Andres Marin, Diego Palacios, Florina Almenarez, and Daniel Diaz-Sanchez. 2016. Comparing Password Management Software: Toward Usable and Secure Enterprise Authentication. *IT Professional* 18, 5 (sep 2016), 34–40. DOI:http://dx.doi.org/10.1109/MITP.2016.81

[12] Dan Ariely, Joel Huber, and Klaus Wertenbroch. 2005. When Do Losses Loom Larger Than Gains? *Journal of Marketing Research* 42, 2 (2005), 134–138.

[13] Dan Ariely and Thomas S. Wallsten. 1995. Seeking Subjective Dominance in Multidimensional Space: An Explanation of the Asymmetric Dominance Effect. *Organizational Behavior and Human Decision Processes* 63, 3 (1995), 223–232. DOI:http://dx.doi.org/10.1006/obhd.1995.1075

[14] Adam J Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *Proceedings of the 4th USENIX Workshop on Offensive technologies (WOOT '13)*. USENIX Association, Washington, DC, USA, 1–10.

[15] Daniel V Bailey, Markus Dürmuth, and Christof Paar. 2014. Statistics on Password Re-use and Adaptive Strength for Financial Accounts. In *Proceedings of the International Conference on Security and Cryptography for Networks*. Springer, Amalfi, Italiy, 218–235. DOI:http://dx.doi.org/10.1007/978-3-319-10879-7_13

[16] Ben F. Barton and Marthalee S. Barton. 1984. User-friendly password methods for computer-mediated information systems. *Computers and Security* 3, 3 (1984), 186–195. DOI:http://dx.doi.org/10.1016/0167-4048(84)90040-3

[17] Ulrich Bayer, Imam Habibi, Davide Balzarotti, Engin Kirda, and Christopher Kruegel. 2009. A view on current malware behaviors. In *Proceedings of the 2nd USENIX conference on Large-scale exploits and emergent threats (LEET '09)*. USENIX Association, Boston, MA, USA, 1–8. https://dl.acm.org/citation.cfm?id=1855684

[18] Frank R Bentley and Ying-Yu Chen. 2015. The Composition and Use of Modern Mobile Phonebooks. In *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems*. ACM, 2749–2758. DOI:http://dx.doi.org/10.1145/2702123.2702182

[19] Chandrasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption. In *Proceedings 2015 Workshop on Usable Security*. Internet Society, Reston, VA, 1–10. DOI:http://dx.doi.org/10.14722/usec.2015.23003

[20] Kemal Bicakci, Nart Bedin Atalay, Mustafa Yuceel, and Paul C van Oorschot. 2012. Exploration and Field Study of a Password Manager Using Icon-Based Passwords. In *Proceedings of International Conference on Financial Cryptography and Data Security*. Springer, Kralendijk, Bonaire, 104–118. DOI:http://dx.doi.org/10.1007/978-3-642-29889-9_9

[21] Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. 2012. Graphical passwords. *Comput. Surveys* 44, 4 (aug 2012), 1–41. DOI:http://dx.doi.org/10.1145/2333112.2333114

[22] Robert Biddle, Mohammad Mannan, Paul C. van Oorschot, and Tara Whalen. 2011. User Study, Analysis, and Usable Security of Passwords Based on Digital Objects. *IEEE Transactions on Information Forensics and Security* 6, 3 (sep 2011), 970–979. DOI:http://dx.doi.org/10.1109/TIFS.2011.2116781

[23] J. Bigun, J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez-Rodriguez. 2005. Combining Biometric Evidence for Person Authentication. In *Advanced Studies in Biometrics*. Number January 2003. Springer Berlin Heidelberg, 1–18. DOI:http://dx.doi.org/10.1007/11493648_1

[24] Matt Bishop and Daniel V. Klein. 1995. Improving system security via proactive password checking. *Computers & Security* 14, 3 (1995), 233–249. DOI:http://dx.doi.org/10.1016/0167-4048(95)00003-Q

[25] Jeremiah Blocki, Anupam Datta, and Joseph Bonneau. 2016. Differentially Private Password Frequency Lists. In *Proceedings 2016 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA, USA, 21–24. DOI:http://dx.doi.org/10.14722/ndss.2016.23328

[26] Jeremiah Blocki, Ben Harsha, and Samson Zhou. 2017. On the Economics of Offline Password Cracking. (2017).

[27] Jeremiah Blocki, Saranga Komanduri, Ariel D Procaccia, and O R Sheffet. 2013. Optimizing Password Composition Policies. In *Proceedings of the fourteenth ACM conference on Electronic commerce*. ACM, Philadelphia, Pennsylvania, USA, 105–122. DOI:http://dx.doi.org/10.1145/2482540.2482552

[28] Greg E. Blonder. 1996. Graphical password. (1996). https://www.google.com/patents/US5559961

[29] Hristo Bojinov, Elie Bursztein, Xavier Boyen, and Dan Boneh. 2010. Kamouflage: Loss-Resistant Password Management. In *Proceedings of ESORICS*, Dimitris Gritzalis, Bart Preneel, and Marianthi Theoharidou (Eds.). Springer Berlin Heidelberg, Athens, Greece, 286–302. DOI:http://dx.doi.org/10.1007/978-3-642-15497-3_18

[30] Joseph Bonneau. 2012a. *Guessing human-chosen secrets*. PhD Thesis.

[31] Joseph Bonneau. 2012b. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *Proceedings - IEEE Symposium on Security and Privacy*. IEEE Comput. Soc, 538–552. DOI:http://dx.doi.org/10.1109/SP.2012.49

[32] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. 2015. Secrets, Lies, and Account Recovery. In *Proceedings of the 24th International Conference on World Wide Web - WWW '15*. ACM Press, Florence, Italy, 141–150. DOI:http://dx.doi.org/10.1145/2736277.2741691

[33] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE, San Francisco, CA, USA, 553–567. DOI:http://dx.doi.org/10.1109/SP.2012.44

[34] Joseph Bonneau, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano. 2015. Passwords and the Evolution of Imperfect Authentication. *Commun. ACM* 58, 7 (2015), 78–87. DOI: http://dx.doi.org/10.1145/2699390

[35] Joseph Bonneau and Stuart Schechter. 2014. Towards Reliable Storage of 56-bit Secrets in Human Memory. In *Proceedings of the 23rd USENIX Security Symposium*. USENIX Association, San Diego, CA, USA, 607–623. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/bonneau

[36] Joseph Bonneau and Ekaterina Shutova. 2012. Linguistic Properties of Multi-word Passphrases. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Vol. 7398 LNCS. Springer, 1–12. DOI: http://dx.doi.org/10.1007/978-3-642-34638-5_1

[37] Serdar Boztas. 1999. *Entropies, Guessing, and Cryptography*. Technical Report 6. Department of Mathematics, Royal Melbourne Institute, Melbourne, Australia.

[38] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. 2011. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security and Privacy* 9, 2 (2011), 18–26. DOI:http://dx.doi.org/10.1109/MSP.2010.198

[39] Sacha Brostoff and MA Sasse. 2003. "Ten strikes and you're out": Increasing the number of login attempts can improve password usability. *In Proceedings of CHI 2003* (2003), 1–4. http://discovery.ucl.ac.uk/19826/

[40] Sacha Brostoff and M Angela Sasse. 2000. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In *People and Computers XIV — Usability or Else!* Springer London, London, 405–424. DOI:http://dx.doi.org/10.1007/978-1-4471-0515-2_27

[41] Alan S. Brown, Elisabeth Bracken, Sandy Zoccoli, and King Douglas. 2004. Generating and remembering passwords. *Applied Cognitive Psychology* 18, 6 (sep 2004), 641–651. DOI:http://dx.doi.org/10.1002/acp.1014

[42] R. Brunelli and D. Falavigna. 1995. Person identification using multiple cues. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 17, 10 (oct 1995), 955–966. DOI: http://dx.doi.org/10.1109/34.464560

[43] A. Buchoux and N.L. Clarke. 2008. Deployment of keystroke analysis on a Smartphone. In *Proceedings of 6th Australian Information Security Management Conference*. Edith Cowan University, Perth, Australia, 29–39. DOI:http://dx.doi.org/10.4225/75/57b55a56b876a

[44] Bundeskriminalamt. 2016. *Cybercrime - Bundeslagebild 2016*. Technical Report. Wiesbaden. 30 pages. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html

[45] Mark Burnett and Dave Kleiman. 2005. Perfect Passwords. *Perfect Passwords* (2005), 107–112. DOI:http://dx.doi.org/10.1016/B978-159749041-2/50012-6

[46] William E. Burr, Donna F. Dodson, and W. Timothy Polk. 2004. Electronic Authentication Guideline. *Special Publication* 800, 63 (2004), 46–64. https://csrc.nist.gov/publications/detail/sp/800-63/ver-10/archive/2004-06-30

[47] Xavier De Carné De Carnavalet and Mohammad Mannan. 2014. From Very Weak to Very Strong : Analyzing Password-Strength Meters. In *Proceedings of the Network and Distributed System Security Symposium (NDSS'14)*. San Diego, CA, USA, 23–26. DOI:http://dx.doi.org/10.14722/ndss.2014.23268

[48] Nancy J. Carter. 2015. Graphical Passwords for Older Computer Users. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology - UIST '15 Adjunct*. ACM Press, Charlotte, NC, USA, 29–32. DOI:http://dx.doi.org/10.1145/2815585.2815593

[49] Claude Castelluccia, Markus Duermuth, Maximilian Golla, and Fatma Deniz. 2017. Towards Implicit Visual Memory-Based Authentication. In *Proceedings 2017 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA, USA, 1–16. DOI:http://dx.doi.org/10.14722/ndss.2017.23292

[50] Sonia Chiasson, Alain Forget, Robert Biddle, and P C van Oorschot. 2008. Influencing users towards better passwords: Persuasive Cued Click-Points. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction*. British Computer Society, Liverpool, United Kingdom, 121–130. http://dl.acm.org/citation.cfm?id=1531514.1531531

[51] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P. C. van Oorschot, and Robert Biddle. 2009. Multiple password interference in text passwords and click-based graphical passwords. In *Proceedings of the 16th ACM conference on Computer and communications security - CCS '09*. ACM Press, Chicago, Illinois, USA, 500–512. DOI:http://dx.doi.org/10.1145/1653662.1653722

[52] Sonia Chiasson and P. C. van Oorschot. 2015. Quantifying the security advantage of password expiration policies. *Designs, Codes and Cryptography* 77, 2-3 (dec 2015), 401–408. DOI:http://dx.doi.org/10.1007/s10623-015-0071-9

[53] Sonia Chiasson, Paul C. Van Oorschot, and Robert Biddle. 2006. A Usability Study and Critique of Two PasswordManagers. In *Proceedings of the 15th conference on USENIX Security Symposium*. USENIX Association, Berkeley, CA, USA, 1–16. http://dl.acm.org/citation.cfm?id=1267336.1267337

[54] Sonia Chiasson, P. C. van Oorschot, and Robert Biddle. 2007. Graphical Password Authentication Using Cued Click Points. In *Proceedings of the 12th European Symposium On Research In Computer Security (ESORICS '12)*. Vol. 4734. Springer, Dresden, Germany, 359–374. DOI:http://dx.doi.org/10.1007/978-3-540-74835-9_24

[55] Yu-Kai Chou. 2015. *Actionable gamification : beyond points, badges, and leaderboards*. CreateSpace Independent Publishing Platform. 499 pages.

[56] Robert B. Cialdini. 2003. Crafting normative messages to protect the environment. *Current Directions in Psychological Science* 12, 4 (2003), 105–109. DOI:http://dx.doi.org/10.1111/1467-8721.01242

[57] Robert B. Cialdini. 2007. *Influence: The Psychology of Persuasion*. Vol. 55. Harper-Collins. 339 pages.

[58] Ashley Colley, Tobias Seitz, Tuomas Lappalainen, Matthias Kranz, and Jonna Häkkilä. 2016. Extending the Touchscreen Pattern Lock Mechanism with Duplicated and Temporal Codes. *Advances in Human-Computer Interaction* 2016, 8762892 (2016), 1–11. DOI:http://dx.doi.org/10.1155/2016/8762892

[59] Art Conklin, Glenn Dietrich, and Diane Walz. 2004. Password-based authentication: a system perspective. In *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*. IEEE, Big Island, HI, USA, 1–10. DOI:http://dx.doi.org/10.1109/HICSS.2004.1265412

[60] Paul T. Costa and Robert R. McCrae. 1992. Revised NEO personality inventory (NEO PI-R) and NEO five-factor inventory (NEO FFI): Professional manual. *Psychological Assessment Resources* 3 (1992), 101. DOI:http://dx.doi.org/10.1037//1040-3590.4.1.5

[61] Lynne Coventry, Pam Briggs, Debora Jeske, and Aad Van Moorsel. 2014. SCENE : A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment. In *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience* (8517 ed.), Aaron Marcus (Ed.). Springer International Publishing, 229–239. DOI:http://dx.doi.org/10.1007/978-3-319-07668-3_23

[62] Lorrie Faith Cranor. 2008. A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*. USENIX Association, San Francisco, CA, USA, 1:1–1:15. http://portal.acm.org/citation.cfm?id=1387650

[63] Heather Crawford. 2010. Keystroke dynamics: Characteristics and opportunities. *PST 2010: 2010 8th International Conference on Privacy, Security and Trust* (2010), 205–212. DOI:http://dx.doi.org/10.1109/PST.2010.5593258

[64] CSID. 2012. *Consumer Survey: Password Habits, A study among American consumers*. Technical Report September. CSID. 10 pages. http://www.csid.com/wp-content/uploads/2012/09/CS

[65] James E. Cutting and Lynn T. Kozlowski. 1977. Recognizing friends by their walk: Gait perception without familiarity cues. *Bulletin of the Psychonomic Society* 9, 5 (1977), 353–356. DOI:http://dx.doi.org/10.3758/BF03337021

[66] Ioannis G. Damousis, Dimitrios Tzovaras, and Evangelos Bekiaris. 2008. Unobtrusive Multimodal Biometric Authentication: The HUMABIO Project Concept. *EURASIP Journal on Advances in Signal Processing* 2008, 1 (dec 2008), 265767. DOI:http://dx.doi.org/10.1155/2008/265767

[67] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and Xf Wang. 2014a. The Tangled Web of Password Reuse. February (2014), 23–26. http://www.jbonneau.com/doc/DBCBW14-NDSS-tangled

[68] Sauvik Das, THJ Kim, LA Dabbish, and JI Hong. 2014b. The Effect of Social Influence on Security Sensitivity. In *Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS'14)*. 143–157. http://cmuchimps.org/uploads/publication/paper/147/the

[69] Darren Davis, Fabian Monrose, and Michael K Reiter. 2004. On user choice in graphical password schemes. In *Proceedings of the 13th conference on USENIX Security Symposium - Volume*

13. USENIX Association, San Diego, CA, USA, 1–13. http://dl.acm.org/citation.cfm?id=1251375.1251386

[70] Antonella De Angeli, Mike Coutts, Lynne Coventry, Graham I. Johnson, David Cameron, and Martin H. Fischer. 2002. VIP: A Visual Approach to User Authentication. In *Proceedings of the Working Conference on Advanced Visual Interfaces - AVI '02*. ACM Press, Trento, Italy, 316–323. DOI:http://dx.doi.org/10.1145/1556262.1556312

[71] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. 2005. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human Computer Studies* 63, 1-2 (2005), 128–152. DOI:http://dx.doi.org/10.1016/j.ijhcs.2005.04.020

[72] Xavier de Carné de Carnavalet and Mohammad Mannan. 2015. A Large-Scale Evaluation of High-Impact Password Strength Meters. *ACM Transactions on Information and System Security* 18, 1 (2015), 1–31. DOI:http://dx.doi.org/10.1145/2739044

[73] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. Touch me once and i know it's you!. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI '12*. ACM Press, Austin, TX, USA, 987–996. DOI:http://dx.doi.org/10.1145/2207676.2208544

[74] Alexander De Luca, Alina Hang, Emanuel von Zezschwitz, and Heinrich Hussmann. 2015. I Feel Like I'm Taking Selfies All Day! Towards Understanding Biometric Authentication on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*. ACM Press, Seoul, South Korea, 1411–1414. DOI:http://dx.doi.org/10.1145/2702123.2702141

[75] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now You See Me, Now You Don't – Protecting Smartphone Authentication from Shoulder Surfers. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*. ACM Press, Toronto, ON, Canada, 2937–2946. DOI:http://dx.doi.org/10.1145/2556288.2557097

[76] Alexander De Luca, Katja Hertzschuch, and Heinrich Hussmann. 2010a. ColorPIN. In *Proceedings of the 28th international conference on Human factors in computing systems (CHI '10)*. ACM Press, Atlanta, GA, USA, 1103. DOI:http://dx.doi.org/10.1145/1753326.1753490

[77] Alexander De Luca, Marc Langheinrich, and Heinrich Hussmann. 2010b. Towards Understanding ATM Security – A Field Study of Real World ATM Use. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. ACM, Redmond, WA, USA, 1–10. DOI:http://dx.doi.org/10.1145/1837110.1837131

[78] Alexander De Luca, Emanuel von Zezschwitz, Ngo Dieu Huong Nguyen, Max-Emanuel Maurer, Elisa Rubegni, Marcello Paolo Scipioni, and Marc Langheinrich. 2013. Back-of-device authentication on smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*. ACM Press, Paris, France, 2389–2398. DOI:http://dx.doi.org/10.1145/2470654.2481330

[79] Yves Alexandre De Montjoye, Jordi Quoidbach, Florent Robic, and Alex Pentland. 2013. Predicting personality using novel mobile phone-based metrics. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 7812 LNCS (2013), 48–55. DOI:http://dx.doi.org/10.1007/978-3-642-37210-0_6

[80] Matteo Dell' Amico, Pietro Michiardi, and Yves Roudier. 2010. Password Strength: An Empirical Analysis. In *Proceedings of IEEE INFOCOM*. IEEE, San Diego, CA, USA, 1–9. DOI: http://dx.doi.org/10.1109/INFCOM.2010.5461951

[81] Matteo Dell'Amico and Maurizio Filippone. 2015. Monte Carlo Strength Evaluation: Fast and Reliable Password Checking. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS- '15)*. ACM, Denver, CO, USA, 158–169. DOI: http://dx.doi.org/10.1145/2810103.2813631

[82] Rachna Dhamija and Adrian Perrig. 2000. Déjà Vu: A User Study Using Images for Authentication. In *Proceedings of the 9th USENIX Security Symposium*. USENIX Association, Denver, CO, USA, 45–58.

[83] Rachna Dhamija and J. D. Tygar. 2005. The Battle Against Phishing : Dynamic Security Skins. In *Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS '05)*. ACM, Pittsburgh, PA, USA, 77–88. DOI:http://dx.doi.org/10.1145/1073001.1073009

[84] Rachna Dhamija, J. D. Tygar, and Marti Hearst. 2006. Why Phishing Works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*. ACM, Montréal, Québec, Canada, 581–590. DOI:http://dx.doi.org/10.1145/1124772.1124861

[85] Paul DiGioia and Paul Dourish. 2005. Social navigation as a model for usable security. In *Proceedings of the 2005 symposium on Usable privacy and security - SOUPS '05*. ACM Press, Pittsburgh, PA, USA, 101–108. DOI:http://dx.doi.org/10.1145/1073001.1073011

[86] Paul Dourish, Rebecca E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (nov 2004), 391–401. DOI:http://dx.doi.org/10.1007/s00779-004-0308-5

[87] Paul Dunphy, Andreas P. Heiner, and N. Asokan. 2010. A closer look at recognition-based graphical passwords on mobile devices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*. ACM Press, Redmond, WA, USA, 1. DOI:http://dx.doi.org/10.1145/1837110.1837114

[88] Paul Dunphy and Jeff Yan. 2007. Do background images improve "draw a secret" graphical passwords?. In *Proceedings of the 14th ACM conference on Computer and communications security - CCS '07*. ACM Press, Alexandria, VA, USA, 36–47. DOI:http://dx.doi.org/10.1145/1315245.1315252

[89] David Eargle, John Godfrey, Hsin Miao, Scott Stevenson, Richard Shay, Blase Ur, and Lorrie Cranor. 2015. Poster : You Can Do Better – Motivational Statements in Password-Meter Feedback. In *Symposium on Usable Privacy and Security (SOUPS '15)*. USENIX Association, Ottawa, Canada, 1–2.

[90] Serge Egelman. 2013. My profile is my password, verify me! The Privacy/Convenience Tradeoff of Facebook Connect. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*. ACM Press, Paris, France, 2369–2378. DOI:http://dx.doi.org/10.1145/2470654.2481328

[91] Serge Egelman, Joseph Bonneau, Sonia Chiasson, David Dittrich, and Stuart Schechter. 2012. It's Not Stealing If You Need It: A Panel on the Ethics of Performing Research Using Public Data of Illicit Origin. In *Proceedings of the 3rd Workshop on Ethics in Computer Security Research (WECSR '12)*, Vol. 7398 LNCS. Springer, Bonaire, Special Municipality of The Netherlands, 124–132. DOI:http://dx.doi.org/10.1007/978-3-642-34638-5_11

[92] Serge Egelman, Adrienne Porter Felt, and David Wagner. 2013. Choice Architecture and Smartphone Privacy: There's A Price for That. In *The economics of information security and privacy*, Rainer Böhme (Ed.). Springer, 211–236. DOI:http://dx.doi.org/10.1007/978-3-642-39498-0_10

[93] Serge Egelman, Marian Harbach, and Eyal Peer. 2016. Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS) Serge. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*. ACM Press, San Jose, CA, USA, 5257–5261. DOI:http://dx.doi.org/10.1145/2858036.2858265

[94] Serge Egelman, David Molnar, Nicolas Christin, Alessandro Acquisti, Cormac Herley, and Shriram Krishnamurthi. 2010. Please Continue to Hold: An empirical study on user tolerance of security delays. In *Proceedings (online) of the 9th Workshop on Economics of Information Security*. Cambridge, MA, USA.

[95] Serge Egelman and Eyal Peer. 2015a. Predicting Privacy and Security Attitudes. *Computers and Society: The Newletter of ACM SIGCAS* 45, 1 (2015), 22–28. DOI:http://dx.doi.org/10.1145/2738210.2738215

[96] Serge Egelman and Eyal Peer. 2015b. Scaling the Security Wall - Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*. ACM Press, Seoul, South Korea, 2873–2882. DOI:http://dx.doi.org/10.1145/2702123.2702249

[97] Serge Egelman and Eyal Peer. 2015c. The Myth of the Average User: Improving Privacy and Security Systems through Individualization. In *Proceedings of the New Security Paradigms Workshop (NSPW '15)*. ACM Press, Twente, The Netherlands, 16–28. DOI:http://dx.doi.org/10.1145/2841113.2841115

[98] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. 2013. Does My Password Go Up to Eleven?: The Impact of Password Meters on Password Selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, Paris, France, 2379–2388. DOI:http://dx.doi.org/10.1145/2470654.2481329

[99] Timo Erdelt. 2017. *Untersuchung von Persönlichkeitsfaktoren für Passwortvorgaben*. Bachelor Thesis. Ludwig-Maximilians-Universität München.

[100] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. 2017. An investigation into users' considerations towards using password managers. *Human-centric*

Computing and Information Sciences 7, 1 (2017), 12. DOI:http://dx.doi.org/10.1186/s13673-017-0093-6

[101] Sascha Fahl, Marian Harbach, Yasemin Acar, and Matthew Smith. 2013. On The Ecological Validity of a Password Study. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13)*. 1–15. DOI:http://dx.doi.org/10.1145/2501604.2501617

[102] David C. (Bellcore) Feldmeier and Philip R (Bellcore) Karn. 1990. UNIX Password Security - Ten Years Later. In *Proceedings of Conference on the Theory and Application of Cryptology (CYPTO '89) (Lecture Notes in Computer Science)*, Gilles Brassard (Ed.), Vol. 435. Springer New York, Santa Barbara, CA, USA, 44–63. DOI:http://dx.doi.org/10.1007/0-387-34805-0

[103] Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. 2015. Improving SSL Warnings: Comprehension and Adherence. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI'15)*. ACM, Seoul, South Korea, 2893–2902. DOI:http://dx.doi.org/10.1145/2702123.2702442

[104] Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, Sunny Consolvo, Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Emre Acer, Elisabeth Morant, Sunny Consolvo, and U C Berkeley. 2016. Rethinking Connection Security Indicators. In *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS '16)*. USENIX Association, Denver, CO, USA, 1–14. RethinkingConnectionSecurityIndicatorsAdriennePorterFelt,RobertW.Reeder,AlexAinslie,HelenHarris,andMaxWalker,Google; ChristopherThompson,UniversityofCalifornia,Berkeley; MustafaEmbreAcer,ElisabethMorant,andSunnyConsolvo,Googl

[105] Adrienne Porter Felt, Robert W. Reeder, Hazim Almuhimedi, and Sunny Consolvo. 2014. Experimenting at scale with google chrome's SSL warning. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*. ACM Press, Toronto, ON, Canada, 2667–2670. DOI:http://dx.doi.org/10.1145/2556288.2557292

[106] Andy Field. 2005. *Discovering Statistics Using SPSS*. Vol. 2nd. Sage Publications Ltd. 779 pages. http://www.amazon.com/Discovering-Statistics-Introducing-Statistical-Methods/dp/0761944524

[107] I Flechais, M Jirotka, and Deena Alghamdi. 2013. In the balance in Saudi Arabia: security, privacy and trust. *CHI '13 Extended Abstracts on Human Factors in Computing Systems* (2013), 823–828. DOI:http://dx.doi.org/10.1145/2468356.2468503

[108] Ivan Flechais, Jens Riegelsberger, and Martina Angela Sasse. 2005. Divide and Conquer: The Role of Trust and Assurance in the Design of Secure Socio-Technical Systems. In *Proceedings of the New Security Paradigms Workshop (NSPW '05)*. ACM, 33–41. http://discovery.ucl.ac.uk/19832/

[109] Dinei Florencio and Cormac Herley. 2007. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web - WWW '07*. ACM Press, New York, New York, USA, 657–665. DOI:http://dx.doi.org/10.1145/1242572.1242661

[110] Dinei Florêncio and Cormac Herley. 2010. Where Do Security Policies Come from?. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. ACM, Redmond, WA, USA, 10:1—-10:14. DOI:http://dx.doi.org/10.1145/1837110.1837124

[111] Dinei Florêncio and Cormac Herley. 2013. Where Do All the Attacks Go? In *Economics of Information Security and Privacy III*. Springer New York, New York, NY, 13–33. DOI: http://dx.doi.org/10.1007/978-1-4614-1981-5_2

[112] Dinei Florêncio, Cormac Herley, and Baris Coskun. 2007. Do strong web passwords accomplish anything? *Security* (2007), 10. http://portal.acm.org/citation.cfm?id=1361419.1361429

[113] Dinei Florêncio, Cormac Herley, and Paul C Van Oorschot. 2014a. An Administrator's Guide to Internet Password Research. In *Proceedings of the 28th Large Installation System Administration Conference (LISA14)*. USENIX Association, Seattle, WA, USA, 35–52.

[114] Dinei Florêncio, Cormac Herley, and Paul C. Van Oorschot. 2014b. Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. In *Proceedings of USENIX Security Symposium*. USENIX Association, San Diego, CA, USA, 575–590. https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-florencio.pdf

[115] Dinei Florêncio, Cormac Herley, and Paul C. Van Oorschot. 2016. Pushing on string: The Don't Care Region of Password Strength. *Commun. ACM* 59, 11 (oct 2016), 66–74. DOI: http://dx.doi.org/10.1145/2934663

[116] BJ Fogg. 2009. A Behavior Model for Persuasive Design. In *Proceedings of the 4th International Conference on Persuasive Technology - Persuasive '09*. ACM Press, Claremont, CA, USA, 1–7. DOI:http://dx.doi.org/10.1145/1541948.1541999

[117] B. J. Fogg. 2003. *Persuasive Technology: Using Computers to Change What We Think and Do*. Morgan Kaufmann, San Francisco, CA, USA.

[118] B. J. Fogg, Jonathan Marshall, Othman Laraki, Alex Osipovich, Chris Varma, Nicholas Fang, Jyoti Paul, Akshay Rangnekar, John Shon, Preeti Swani, Marissa Treinen, and Cordura Hall. 2001. What Makes Web Sites Credible ? A Report on a Large Quantitative Study. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '01)*. 61–68. DOI:http://dx.doi.org/10.1145/365024.365037

[119] Alain Forget and Robert Biddle. 2008. Memorability of Persuasive Passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*. ACM, Florence, Italy, 3759. DOI:http://dx.doi.org/10.1145/1358628.1358926

[120] Alain Forget, Sonia Chiasson, and Robert Biddle. 2007a. Helping users create better passwords: Is this the right approach?. In *Proceedings of the 3rd symposium on Usable privacy and security - SOUPS '07*. ACM Press, Pittsburg, PA, USA, 151–154. DOI:http://dx.doi.org/10.1145/1280680.1280703

[121] Alain Forget, Sonia Chiasson, and Robert Biddle. 2007b. Persuasion as Education for Computer Security. In *Proceedings of E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*. Association for the Advancement of Computing in Education (AACE), Chesapeake, VA, 822–829.

[122] Alain Forget, Sonia Chiasson, and Robert Biddle. 2015. Choose Your Own Authentication. In *Proceedings of the New Security Paradigms Workshop (NSPW '15)*. ACM, Twente, The Netherlands. DOI:http://dx.doi.org/10.1145/1235

[123] Alain Forget, Sonia Chiasson, P C Van Oorschot, and Robert Biddle. 2008a. Improving Text Passwords Through Persuasion. In *Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS '08)*. ACM, New York, NY, USA, 1–12. DOI:http://dx.doi.org/10.1145/1408664.1408666

[124] Alain Forget, Sonia Chiasson, Paul C. Van Oorschot, and Robert Biddle. 2008b. Persuasion for stronger passwords. In *Proceedings of the 3rd International Conference on Persuasive Technology for Human Well-Being*. Springer Berlin Heidelberg, Oulu, Finland, 140–150. http://www.scs.carleton.ca/

[125] Marlena R Fraune, Kevin A Juang, Joel S Greenstein, Kapil Chalil Madathil, and Reshmi Koikkara. 2013. Employing User-Created Pictures to Enhance the Recall of System-Generated Mnemonic Phrases and the Security of Passwords. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 57, 1 (sep 2013), 419–423. DOI:http://dx.doi.org/10.1177/1541931213571091

[126] Steven Furnell and Rawan Esmael. 2017. Evaluating the effect of guidance and feedback upon password compliance. *Computer Fraud and Security* 2017, 1 (2017), 5–10. DOI:http://dx.doi.org/10.1016/S1361-3723(17)30005-2

[127] Vaibhav Garg and Jean Camp. 2013. Heuristics and Biases: Implications for Security Design. *IEEE Technology and Society Magazine* 32, 1 (2013), 73–79. DOI:http://dx.doi.org/10.1109/MTS.2013.2241294

[128] Morrie Gasser. 1975. *A Random Word Generator for Pronounceable Passwords*. Technical Report. The MITRE Corporation, Bedford, Massachusettss. 193 pages. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA017676

[129] Shirley Gaw and Edward Felten. 2005. Reuse and Recycle : Online Password Management. In *Extended Abstracts of the Symposium on Usable Privacy and Security (SOUPS '05)*. CMU Usable Privacy and Security Laboratory, Pittsburg, PA, USA, 42–43.

[130] Shirley Gaw and Edward W. Felten. 2006. Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security (SOUPS '06)*. ACM, New York, NY, USA, 44–55. DOI:http://dx.doi.org/10.1145/1143120.1143127

[131] Paul Gerber, Marco Ghiglieri, Birgit Henhapl, Oksana Kulyk, Karola Marky, Peter Mayer, Benjamin Reinheimer, and Melanie Volkamer. 2018. Human Factors in Security. In *Sicherheitskritische Mensch-Computer-Interaktion*. Springer Fachmedien Wiesbaden, Wiesbaden, 83–98. DOI:http://dx.doi.org/10.1007/978-3-658-19523-6_5

[132] Jurijs Girtakovskis, Ken Jacobi, David Kennerley, Kiran Kumar, Grayson Milbourne, Tyler Moffitt, Cameron Palan, and Steve Snyder. 2017. *The Webroot 2017 Annual Threat Report*. Technical Report. Webroot, Broomfield, CO, USA. 24 pages. https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8114/8883/6877/Webroot

[133] Jeffrey Goldberg. 2015. Unspeakable Passwords - Pronounceable or Random Words (Talk). (2015).

[134] Maximilian Golla, Dennis Detering, and Markus Dürmuth. 2017. EmojiAuth : Quantifying the Security of Emoji-based Authentication. In *USEC 2017*. Internet Society, San Jose, CA, USA, 1–13. DOI:http://dx.doi.org/10.14722/usec.2017.23024

[135] Samuel D. Gosling, Peter J. Rentfrow, and William B. Swann. 2003. A very brief measure of the Big-Five personality domains. *Journal of Research in Personality* 37, 6 (2003), 504–528. DOI:http://dx.doi.org/10.1016/S0092-6566(03)00046-1

[136] Jeff Gothelf and Josh Seiden. 2013. *Lean UX*. 1–151 pages. DOI:http://dx.doi.org/10.1017/CBO9781107415324.004

[137] C L Grady, A R McIntosh, M N Rajah, and F I Craik. 1998. Neural correlates of the episodic encoding of pictures and words. *Proceedings of the National Academy of Sciences USA* 95, 5 (1998), 2703–2708. DOI:http://dx.doi.org/10.1073/pnas.95.5.2703

[138] Adam M Grant. 2013. Rethinking the Extraverted Sales Ideal: The Ambivert Advantage. *Psychological Science* 24, 6 (jun 2013), 1024–1030. DOI:http://dx.doi.org/10.1177/0956797612463706

[139] Rachel Greenstadt and Jacob Beal. 2008. Cognitive Security for Personal Devices. In *Proceedings of the 1st ACM workshop on Workshop on AISec - AISec '08*. ACM Press, Alexandria, VA, USA, 27–30. DOI:http://dx.doi.org/10.1145/1456377.1456383

[140] Thomas Groß, Kovila Coopamootoo, and Amina Al-jabri. 2016a. *Effect of Cognitive Depletion on Password Choice*. Technical Report September. Newcastle University, Newcastle, UK. 1–16 pages. https://www.usenix.org/system/files/conference/soups2016/way

[141] Thomas Groß, Kovila P.L. Coopamootoo, and Amina Al-Jabri. 2016b. Effect of Cognitive Effort on Password Choice. In *Symposium on Usable Privacy and Security - Posters*. USENIX Association, Denver, CO, USA, 1–2.

[142] Iwan Gulenko. 2014. Improving passwords: influence of emotions on security behaviour. *Information Management & Computer Security* 22, 2 (2014), 167–178. DOI:http://dx.doi.org/10.1108/IMCS-09-2013-0068

[143] Yimin Guo and Zhenfeng Zhang. 2017. LPSE: lightweight password-strength estimation for password meters. *Computers & Security* (2017). DOI:http://dx.doi.org/10.1016/j.cose.2017.07.012

[144] Hana Habib, Jessica Colnago, William Melicher, Blase Ur, Sean M. Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Cranor. 2017. Password Creation in the Presence of Blacklists. In *Proceedings of the 2017 Workshop on Usable Security*. Internet Society, San Diego, CA, USA, 11. DOI:http://dx.doi.org/10.14722/usec.2017.23043

[145] J Alex Halderman, Brent Waters, and Edward W Felten. 2005. A convenient method for securely managing passwords. In *Proceedings of the 14th international conference on World Wide Web - WWW '05*. ACM Press, Chiba, Japan, 471. DOI:http://dx.doi.org/10.1145/1060745.1060815

[146] Tzipora Halevi, James Lewis, and Nasir Memon. 2013. A pilot study of cyber security and privacy related behavior and personality traits. In *WWW 2013 Companion - Proceedings of the 22nd International Conference on World Wide Web*. 737–744. DOI:http://dx.doi.org/10.1145/2487788.2488034

[147] Tzipora Halevi, Nasir Memon, and Oded Nov. 2015. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. *SSRN Electronic Journal* (2015). DOI:http://dx.doi.org/10.2139/ssrn.2544742

[148] Juho Hamari, Jonna Koivisto, and Tuomas Pakkanen. 2014. Do persuasive technologies persuade? - A review of empirical studies. In *Lecture Notes in Computer Science*, Vol. 8462 LNCS. 118–136. DOI:http://dx.doi.org/10.1007/978-3-319-07127-5_11

[149] Alina Hang. 2015. *Exploiting Autobiographical Memory for Fallback Authentication on Smartphones*. Dissertation. Ludwig-Maximilians-Universität München.

[150] Alina Hang, Alexander De Luca, Katharina Frison, Emanuel von Zezschwitz, Massimo Tedesco, Marcel Kockmann, and Heinrich Hussmann. 2013. Travel Routes or Geography Facts? An Evaluation of Voice Authentication User Interfaces. In *Proceedings of INTERACT*, Vol. 8119 LNCS. Springer, Cape Town, South Africa, 468–475. DOI:http://dx.doi.org/10.1007/978-3-642-40477-1_29

[151] SMT Haque, Shannon Scielzo, and Matthew Wright. 2014a. Applying Psychometrics to Measure User Comfort when Constructing a Strong Password. In *Symposium on Usable Privacy and Security (SOUPS)*. Menlo Park, CA, USA, 231–242. https://www.usenix.org/system/files/conference/soups2014/soups14-paper-haque.pdf

[152] S. M Taiabul Haque, Matthew Wright, and Shannon Scielzo. 2014b. Hierarchy of users' web passwords: Perceptions, practices and susceptibilities. *International Journal of Human Computer Studies* 72, 12 (2014), 860–874. DOI:http://dx.doi.org/10.1016/j.ijhcs.2014.07.007

[153] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *SOUPS '14: Proceedings of the Tenth Symposium On Usable Privacy and Security*. 213–230. https://www.usenix.org/conference/soups2014/proceedings/presentation/harbach

[154] Garett Hardin. 1968. The Tragedy of the Commons. *Science* 162, 3859 (1968), 1243–8. DOI:http://dx.doi.org/10.1126/science.162.3859.1243

[155] James A Haskett. 1984. Pass-algorithms: a user validation scheme based on knowledge of secret algorithms. *Commun. ACM* 27, 8 (1984), 777–781. DOI:http://dx.doi.org/10.1145/358198.358214

[156] Eiji Hayashi, Rachna Dhamija, Nicolas Christin, and Adrian Perrig. 2008. Use Your Illusion. In *Proceedings of the 4th symposium on Usable privacy and security - SOUPS '08*. ACM Press, Pittsburgh, PA, USA, 35–45. DOI:http://dx.doi.org/10.1145/1408664.1408670

[157] Eiji Hayashi and Jason Hong. 2011. A diary study of password usage in daily life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, Vancouver, BC, Canada, 2627–2631. DOI:http://dx.doi.org/10.1145/1978942.1979326

[158] EB Hekler, Predrag Klasnja, JE Froehlich, and MP Buman. 2013. Mind the Theoretical Gap: Interpreting, Using, and Developing Behavioral Theory in HCI Research. http://www.designinghealth.org/uploads/1/3/8/4/13844497/hci

[159] Olaf Henniger, Dirk Scheuermann, and Thomas Kniess. On security evaluation of fingerprint recognition systems. In *Proceedings of the International Biometric Performance Testing Conference (IBPC)*. NIST, Gaithersburg, MD, USA.

[160] Cormac Herley. 2009. So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Proceedings of the New Security Paradigms Workshop (NSPW '09)*. ACM, Oxford, United Kingdom, 133–144. DOI:http://dx.doi.org/10.1145/1719030.1719050

[161] Cormac Herley. 2014. Security, cybercrime, and scale. *Commun. ACM* 57, 9 (sep 2014), 64–71. DOI:http://dx.doi.org/10.1145/2654847

[162] Cormac Herley and Wolter Pieters. 2015. "If you were attacked, you'd be sorry": Counterfactuals as security arguments. In *Proceedings of the New Security Paradigms Workshop on ZZZ - NSPW '15*. ACM Press, Twente, The Netherlands, 112–123. DOI:http://dx.doi.org/10.1145/2841113.2841122

[163] Cormac Herley and Paul Van Oorschot. 2012. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security and Privacy* 10, 1 (2012), 28–36. DOI:http://dx.doi.org/10.1109/MSP.2011.150

[164] Moritz Horsch, Mario Schlipf, Stefen Haas, Johannes Braun, and Johannes Buchmann. 2016. Password Policy Markup Language. In *Proceedings of Open Identify Summit*. Gesellschaft für Informatik, Rome, Italy, 135–147.

[165] Joel Huber, John W. Payne, and Christopher Puto. 1982. Adding Asymmetrically Dominated Alternatives: Violations of Regularity and the Similarity Hypothesis. *Journal of Consumer Research* 9, 1 (1982), 90. DOI:http://dx.doi.org/10.1086/208899

[166] Paul Huber. 2016. *Einfluss des Persönlichkeitstyps auf die Wahrnehmung von Passwortkomplexität*. Bachelor Thesis. Ludwig-Maximilians-Universität München.

[167] Jun Ho Huh, Hyoungshick Kim, Swathi S.V.P. Rayala, Rakesh B. Bobba, and Konstantin Beznosov. 2017. I'm too Busy to Reset my LinkedIn Password: On the Effectiveness of Password Reset Emails. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. ACM Press, Denver, CO, USA, 387–391. DOI:http://dx.doi.org/10.1145/3025453.3025788

[168] Jun Ho Huh, Seongyeol Oh, Hyoungshick Kim, Konstantin Beznosov, Apurva Mohan, and S. Raj Rajagopalan. 2015. Surpass: System-initiated User-replaceable Passwords. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15*. ACM Press, Denver, CO, USA, 170–181. DOI:http://dx.doi.org/10.1145/2810103.2813622

[169] Ahsan Imran. 2015. *A Comparison of Password Authentication Between Children and Adults*. Master Thesis. Carleton University, Ottawa, Ontario.

[170] Philip Inglesant and Martina Angela Sasse. 2010. The True Cost of Unusable Password Policies: Password Use in the Wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, Atlanta, GA, USA, 383–392. DOI:http://dx.doi.org/10.1145/1753326.1753384

[171] Blake Ives, Kenneth R. Walsh, and Helmut Schneider. 2004. The Domino Effect of Password Reuse. *Commun. ACM* 47, 4 (apr 2004), 75–78. DOI:http://dx.doi.org/10.1145/975817.975820

[172] Sheena S. Iyengar and Mark R. Lepper. 2000. When Choice is Demotivating: Can One Desire Too Much of a Good thing? *Journal of Personality and Social Psychology* 79, 6 (2000), 995–1006. DOI:http://dx.doi.org/10.1037/0022-3514.79.6.995

[173] David Jaeger, Chris Pelchen, Hendrik Graupner, Feng Cheng, and Christoph Meinel. 2016. Analysis of Publicly Leaked Credentials and the Long Story of Password (Re-)use. In *Proceedings of the 11th International Conference on Passwords (PASSWORDS2016)*. Springer, Bochum, Germany, 1–19.

[174] Markus Jakobsson. 2014. *How to Wear Your Password*. Technical Report. Qualcomm Research. http://www.markus-jakobsson.com/wp-content/uploads/WP-us-14-Jakobsson-HowToWearYourPassword.pdf

[175] Markus Jakobsson and Mayank Dhiman. 2013. The Benefits of Understanding Passwords. In *Mobile Authentication* (2 ed.). Springer, 5–24. DOI:http://dx.doi.org/10.1007/978-1-4614-4878-5_2

[176] Markus Jakobsson, Elaine Shi, Philippe Golle, and Richard Chow. 2009. Implicit authentication for mobile devices. In *Proceedings of the 4th USENIX conference on Hot topics in security (HotSec'09)*. USENIX Association, Montreal, Canada, 1–6.

[177] Anthony Jameson, Silvia Gabrielli, Per Ola Kristensson, Katharina Reinecke, Federica Cena, Cristina Gena, and Fabiana Vernero. 2011. How can we support users' preferential choice? *Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems - CHI EA '11* (2011), 409. DOI:http://dx.doi.org/10.1145/1979742.1979620

[178] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K Reiter, and Aviel D Rubin. 1999. The Design and Analysis of Graphical Passwords. In *Proceedings of the 8th USENIX Security Symposium*, Vol. 8. USENIX Association, Washington, DC, USA, 1–14. DOI:http://dx.doi.org/10.1109/ICCIIS.2010.35

[179] Debora Jeske, Lynne Coventry, and Pam Briggs. 2014. Nudging whom how : IT proficiency , impulse control and secure behaviour. In *Proceedings of the CHI Workshop on Personalizing Behavior Change Technologies*. Toronto, ON, Canada, 1–4.

[180] Daniel Kahneman. 2003. Maps of bounded rationality: Psychology for behavioral economics. *American Economic Review* 93, 5 (2003), 1449–1475. DOI:http://dx.doi.org/10.1257/000282803322655392

[181] Daniel Kahneman. 2011. *Thinking, fast and slow*. 499 pages. https://books.google.de/books?id=ZuKTvERuPG8C

[182] Daniel Kahnemann and Shane Frederick. 2002. Heuristics of Intuitive Judgment: Extensions and Applications. In *Heuristics of Intuitive Judgment: Extensions and Applications*, D. Griffin T. Gilovich and D. Kahneman (Eds.). Cambridge University Press, New York, New York, USA, 1–30.

[183] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My data just goes everywhere": User mental models of the internet and implications for privacy and security. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '15)*. USENIX Association, Ottawa, Canada, 39–52. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-kang.pdf

[184] Christina Katsini, Nikolaos Avouris, Christos Fidas, George Samaras, and Marios Belk. 2017. Influences of Users' Cognitive Strategies on Graphical Password Composition. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '17)*. ACM, Denver, CO, USA, 2698–2705. DOI:http://dx.doi.org/10.1145/3027063.3053217

[185] Joseph 'Jofish' Kaye. 2011. Self-reported password sharing strategies. In *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*. ACM Press, Vancouver, BC, Canada, 2619. DOI:http://dx.doi.org/10.1145/1978942.1979324

[186] Mark Keith, Benjamin Shao, and Paul Steinbart. 2009. A Behavioral Analysis of Passphrase Design and Effectiveness. *Journal of the Association for Information Systems* 10, 2 (2009), 63–89. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1492

[187] Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio Lopez. 2012a. Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. In *2012 IEEE Symposium on Security and Privacy*. IEEE, San Francisco, CA, USA, 523–537. DOI:http://dx.doi.org/10.1109/SP.2012.38

[188] Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio López. 2012b. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *Proceedings - IEEE Symposium on Security and Privacy*. 523–537. DOI:http://dx.doi.org/10.1109/SP.2012.38

[189] Warut Khern-am nuai, Weining Yang, and Ninghui Li. 2017. Using Context-Based Password Strength Meter to Nudge Users' Password Generating Behavior: A Randomized Experiment. In *SSRN Electronic Journal*. 27. DOI:http://dx.doi.org/10.24251/HICSS.2017.071

[190] Ran Kivetz, Oleg Urminsky, and Yuhuang Zheng. 2006. The Goal-Gradient Hypothesis Resurrected: Purchase Acceleration, Illusionary Goal Progress, and Customer Retention. *Journal of Marketing Research* 43, 1 (2006), 39–58. DOI:http://dx.doi.org/10.1509/jmkr.43.1.39

[191] Bart P Knijnenburg, Alfred Kobsa, and Hongxia Jin. 2013. Preference-based location sharing: Are More Privacy Options Really Better?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*. ACM Press, Paris, France, 2667–2676. DOI:http://dx.doi.org/10.1145/2470654.2481369

[192] John Kohl and Clifford Neuman. 1993. The Kerberos Network Authentication Service (V5). (1993). http://www.rfc-editor.org/rfc/rfc1510.txt

[193] Saranga Komanduri. 2016. *Modeling the Adversary to Evaluate Password Strength With Limited Samples*. Dissertation. Carnegie Mellon University.

[194] Saranga Komanduri, Richard Shay, Lorrie Faith Cranor, Cormac Herley, and Stuart Schechter. 2014. Telepathwords: Preventing Weak Passwords by Reading Users' Minds. In *23rd USENIX Security Symposium (USENIX Security 14)*. USENIX Association, San Diego, CA, USA, 591–606. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/komanduri

[195] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. 2011. Of passwords and people. In *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*. 2595. DOI:http://dx.doi.org/10.1145/1978942.1979321

[196] Stefan Korff and Rainer Böhme. 2014. Too Much Choice: End-User Privacy Decisions in the Context of Choice Proliferation. In *Symposium on Usable Privacy and Security (SOUPS '14)*. 69–87. https://www.usenix.org/system/files/soups14-paper-korff.pdf

[197] Vijay Kothari, Ross Koppel, Jim Blythe, and Sean Smith. 2017. Password Logbooks and What Their Amazon Reviews Reveal About Their Users' Motivations, Beliefs, and Behaviors. In *Proceedings 2nd European Workshop on Usable Security*. Internet Society, Paris, France, 10. DOI:http://dx.doi.org/10.14722/eurousec.2017.23018

[198] Lydia Kraus, Robert Schmidt, Marcel Walch, Florian Schaub, and Sebastian Möller. 2017. On the Use of Emojis in Mobile Authentication. In *IFIP Advances in Information and Communication Technology*. Vol. 502. Springer, Cham, 265–280. DOI:http://dx.doi.org/10.1007/978-3-319-58469-0_18

[199] Christien Kroeze and Martin S. Olivier. 2012. Gamifying authentication. In *2012 Information Security for South Africa*. IEEE, Johannesburg, Gauteng, South Africa, 1–8. DOI:http://dx.doi.org/10.1109/ISSA.2012.6320439

[200] Kat Krol, Jonathan M Spring, Simon Parkin, and M Angela Sasse. 2016. Towards robust experimental design for user studies in security and privacy. In *Learning from Authoritative Security Experiment Results (LASER '16)*. USENIX Association, 21–32.

[201] Cynthia Kuo, Sasha Romanosky, and Lorrie Faith Cranor. 2006. Human Selection of Mnemonic Phrase-Based Passwords. In *Proceedings of the second Symposium on Usable Privacy and Security (SOUPS '06)*. 67–78. DOI:http://dx.doi.org/10.1145/1143120.1143129

[202] Stanley A. Kurzban. 1985. Easily Remembered Passphrases - A Better Approach. *ACM SIGSAC Review* 3, 2-4 (sep 1985), 10–21. DOI:http://dx.doi.org/10.1145/1058406.1058408

[203] LastPass. 2016. *The Password Paradox and why our Personalities will get us Hacked*. Technical Report. 1–6 pages. http://prod.cdata.app.sprinklr.com/DAM/434/LastPass

[204] Yue Li, Haining Wang, and Kun Sun. 2017. Personal Information in Passwords and Its Security Implications. *IEEE Transactions on Information Forensics and Security* 12, 10 (oct 2017), 2320–2333. DOI:http://dx.doi.org/10.1109/TIFS.2017.2705627

[205] Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song. 2014. The Emperor's New Password Manager: Security Analysis of Web-based Password Managers. In *Proceedings of the*

23rd USENIX Security Symposium (USENIX Security 14). USENIX Association, San Diego, CA, USA, 465–479. http://devd.me/papers/pwdmgr-usenix14.pdf

[206] William Lidwell, Kritina Holden, and Jill Butler. 2003. *Universal Principles of Design*. Vol. 2007. Rockport Publishers. 216 pages. DOI:http://dx.doi.org/10.1007/s11423-007-9036-7

[207] Eric Lin, Saul Greenberg, Eileah Trotter, David Ma, and John Aycock. 2011. Does domain highlighting help people identify phishing sites?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 2075–2084. DOI:http://dx.doi.org/10.1145/1978942.1979244

[208] David Llewellyn-jones and Graham Rymer. 2016. Cracking PwdHash: A Bruteforce Attack on Client-side Password Hashing. In *Proceedings of the 11th International Conference on Passwords*. Springer, Bochum, Germany, 1–19.

[209] Dan Lockton. 2012. Cognitive Biases, Heuristics and Decision-Making in Design for Behaviour Change. (2012). http://papers.ssrn.com/sol3/papers.cfm?abstract

[210] Dan Lockton, David Harrison, and Neville a Stanton. 2010. The Design with Intent Method: A design tool for influencing user behaviour. *Applied Ergonomics* 41, 3 (may 2010), 382–392. DOI:http://dx.doi.org/10.1016/j.apergo.2009.09.001

[211] Ijlal Loutfi and Audun Jøsang. 2015. Passwords are not always stronger on the other side of the fence. In *Proceedings of the Network and Distributed System Security Conference, USEC Workshop*. Internet Society, San Diego, CA, USA, 1–10. DOI:http://dx.doi.org/10.14722/usec.2015.23005

[212] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Sven Bugiel, and Michael Backes. 2017. *Studying the Impact of Managers on Password Strength and Reuse*. Technical Report. 1–20 pages. http://arxiv.org/abs/1712.08940

[213] Joseph Maguire and Karen Renaud. 2012. You Only Live Twice or The Years We Wasted Caring about Shoulder-Surfing. In *Proceedings of the 26th Annual BCS Interaction Specialist Group Conference on People and Computers (BCS-HCI '12)*. BISL / ACM, Birmingham, UK, 404–409. http://eprints.gla.ac.uk/71011/

[214] Nathan Malkin, Shriram Krishnamurthi, and David H. Laidlaw. 2013. Waiting Makes the Heart Grow Fonder and the Password Grow Stronger. In *Symposium on Usable Privacy and Security (SOUPS) - Posters*. USENIX Association, Newcastle, UK, 1–2. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.364.14

[215] Fatma AL Maqbali and Chris J Mitchell. 2016. Password Generators: Old Ideas and New. September (2016), 1–20. http://arxiv.org/abs/1607.04421

[216] Emanuela Marasco and Arun Ross. 2014. A Survey on Antispoofing Schemes for Fingerprint Recognition Systems. *Comput. Surveys* 47, 2 (nov 2014), 1–36. DOI:http://dx.doi.org/10.1145/2617756

[217] Simon Marechal. 2008. Advances in password cracking. *Journal in Computer Virology* 4, 1 (2008), 73–81. DOI:http://dx.doi.org/10.1007/s11416-007-0064-y

[218] Davide Marengo, Fabrizia Giannotta, and Michele Settanni. 2017. Assessing personality using emoji: An exploratory study. *Personality and Individual Differences* 112, July (2017), 74–78. DOI:http://dx.doi.org/10.1016/j.paid.2017.02.037

[219] Max-emanuel Maurer, Alexander De Luca, and Sylvia Kempe. 2011a. Using Data Type Based Security Alert Dialogs to Raise Online Security Awareness. In *SOUPS '11 Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, Pittsburg, PA, USA, Paper 2. DOI: http://dx.doi.org/10.1145/2078827.2078830

[220] Max-Emanuel Maurer, Alexander De Luca, and Tobias Stockinger. 2011b. Shining Chrome: Using Web Browser Personas to Enhance SSL Certificate Visualization. In *Proceedings of the international conference on Human-computer interaction (INTERACT'11)*. Springer, Berlin, Heidelberg, 44–51. http://link.springer.com/chapter/10.1007/978-3-642-23768-3

[221] Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur. 2013. Measuring password guessability for an entire university. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13*. ACM Press, New York, New York, USA, 173–186. DOI:http://dx.doi.org/10.1145/2508859.2516726

[222] Daniel McCarney. 2013. *Password Managers: Comparative Evaluation, Design, Implementation and Empirical Analysis*. Ph.D. Dissertation. Carleton University.

[223] Daniel McCarney, David Barrera, Jeremy Clark, Sonia Chiasson, and Paul C. van Oorschot. 2012. Tapas: Design, Implementation, and Usability Evaluation of a Password Manager. In *Proceedings of the 28th Annual Computer Security Applications Conference on - ACSAC '12*. ACM Press, Orlando, FL, USA, 89–99. DOI:http://dx.doi.org/10.1145/2420950.2420964

[224] Robert R. McCrae and Paul T. Costa. 1987. Validation of the Five-Factor Model of Personality Across Instruments and Observers. *Journal of Persoanlity and Social Psychology* 52, 1 (1987), 81–90.

[225] Pete McEvoy and Jeremiah D Still. 2016. Contextualizing Mnemonic Phrase Passwords. In *Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity*. Springer, Cham, Orlando, FL, USA, 295–304. DOI:http://dx.doi.org/10.1007/978-3-319-41932-9_24

[226] William Melicher, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L Mazurek. 2016a. Usability and Security of Text Passwords on Mobile Devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 527–539. DOI:http://dx.doi.org/10.1145/2858036.2858384

[227] William Melicher, Blase Ur, Sean M. Segreti, Saranga Komanduri, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016b. Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks. In *Proceedings of the 25th USENIX Security Symposium*. USENIX Association, Austin, TX, USA, 175–191.

[228] Tehila Minkus and Nasir Memon. 2014. Leveraging Personalization to Facilitate Privacy. (2014). http://papers.ssrn.com/abstract=2448026

[229] Kevin D. Mitnick and William L. Simon. 2002. *The Art of Deception: Controlling the Human Element in Security* (1st editio ed.). Wiley. 352 pages. DOI:http://dx.doi.org/0471237124

[230] Robert Morris and Ken Thompson. 1979. Password Security: A Case History. *Commun. ACM* 22, 11 (1979), 594–597. DOI:http://dx.doi.org/10.1145/359168.359172

[231] Nicole L. Muscanell, Rosanna E. Guadagno, and Shannon Murphy. 2014. Weapons of influence misused: A social influence analysis of why people fall prey to internet scams. *Social and Personality Psychology Compass* 8, 7 (2014), 388–396. DOI:http://dx.doi.org/10.1111/spc3.12115

[232] Arvind Narayanan and Vitaly Shmatikov. 2005. Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff. In *Proceedings of the 12th ACM conference on Computer and communications security - CCS '05*. ACM, Alexandria, VA, USA, 364–372. DOI:http://dx.doi.org/10.1145/1102120.1102168

[233] Mohammad Nauman and Tamleek Ali. 2010. TOKEN: Trustable Keystroke-Based Authentication for Web-Based Applications on Smartphones. In *Communications in Computer and Information Science*. Vol. 76 CCIS. Springer Berlin Heidelberg, 286–297. DOI:http://dx.doi.org/10.1007/978-3-642-13365-7_28

[234] Aline Neumann. 2017. *Effects of Personality on Password Selection*. Bachelor Thesis. Ludwig-Maximilians-Universität München.

[235] Jakob Nielsen. 1994. Enhancing the explanatory power of usability heuristics. In *Proceedings of the SIGCHI conference on Human factors in computing systems celebrating interdependence - CHI '94*. ACM Press, Boston, MA, USA, 152–158. DOI:http://dx.doi.org/10.1145/191666.191729

[236] Chris Nodder. 2013. *Evil By Design* (1 ed.). Wiley, Indianapolis, IN, USA. 322 pages.

[237] Don Norman. 1983. Some Observations on Mental Models. In *Mental Models*. Psychology Press, Chapter 1, 7–14.

[238] Gilbert Notoatmodjo. 2007. *Exploring the ' Weakest Link ': A Study of Personal Password Security*. Master Thesis. University of Auckland, New Zealand.

[239] Kenneth Olmstead and Aaron Smith. 2017. *Americans and Cybersecurity*. Technical Report. Pew Research Center. 42 pages. http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf

[240] Daniel M. Oppenheimer, Tom Meyvis, and Nicolas Davidenko. 2009. Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology* 45, 4 (2009), 867–872. DOI:http://dx.doi.org/10.1016/j.jesp.2009.03.009

[241] J R B Paiva, V M Gomes, and C Morris. 2017. Passfault : an Open Source Tool for Measuring Password Complexity and Strength. In *Proceedings of the 8th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC '17)*. OWASP, Orlando, FL, USA. https://www.owasp.org/images/1/13/Artigo-Passfault.pdf

[242] Allan Paivio, T.B. Rogers, and Padric C. Smythe. 1968. Why are Pictures Easier to Recall Than Words ? *Psychonomic Science* 11, 4 (1968), 137–138. DOI:http://dx.doi.org/10.3758/BF03331011

[243] J.L. Parrish Jr., J.L. Bailey, and J.F. Courtney. 2009. A Personality Based Model for Determining Susceptibility to Phishing Attacks. *Southwest Decision Sciences Institute (SWDSI) annual meeting* October 2015 (2009), 285–296.

[244] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. 2017. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology* 70 (2017), 153–163. DOI:http://dx.doi.org/10.1016/j.jesp.2017.01.006

[245] Sean Peisert, Ed Talbot, and Tom Kroeger. 2013. Principles of authentication. In *Proceedings of the 2013 workshop on New security paradigms workshop - NSPW '13*. ACM Press, Banff, Alberta, Canada, 47–56. DOI:http://dx.doi.org/10.1145/2535813.2535819

[246] John O. Pliam. 2000. On the Incomparability of Entropy and Marginal Guesswork in Brute-Force Attacks. In *Proceedings of Progress in Cryptology - INDOCRYPT 2000*. Springer Berlin Heidelberg, Calcutta, India, 67–79. DOI:http://dx.doi.org/10.1007/3-540-44495-5_7

[247] Martin Prinz. 2017. *Developing a Secure Password-Reuse-Manager*. Master Thesis. Ludwig-Maximilans-Universität München.

[248] Martin Prinz and Tobias Seitz. 2017. Towards a Mental Model of Password Management Software. In *Extended Abstracts of the Symposium on Usable Privacy and Security (SOUPS EA 2017)*. USENIX Association, Santa Clara, CA, USA.

[249] Robert W Proctor, Mei-Ching Lien, Kim-Phuong L Vu, E Eugene Schultz, and Gavriel Salvendy. 2002. Improving Computer Security for Authentication of Users: Influence of Proactive Password Restrictions. *Behavior Research Methods, Instruments, & Computers: A Journal of the Psychonomic Society, Inc* 34, 2 (2002), 163–169. DOI:http://dx.doi.org/10.3758/BF03195438

[250] Niels Provos and David Mazieres. 1999. A future-adaptable password scheme. In *Proceedings of the USENIX Annual Technical Conference*. USENIX Association, Monterey, CA, USA, 1–12. https://www.usenix.org/legacy/event/usenix99/full

[251] Kenneth Radke, Colin Boyd, Juan Gonzalez Nieto, and Laurie Buys. 2013. "Who decides?" Security and Privacy in the Wild. In *Proceedings of the 25th Australian Computer-Human Interaction Conference on Augmentation, Application, Innovation, Collaboration - OzCHI '13*. ACM Press, Adelaide, Australia, 27–36. DOI:http://dx.doi.org/10.1145/2541016.2541043

[252] Beatrice Rammstedt and Oliver P. John. 2005. Kurzversion des Big Five Inventory (BFI-K):. *Diagnostica* 51, 4 (oct 2005), 195–206. DOI:http://dx.doi.org/10.1026/0012-1924.51.4.195

[253] Janet Read, Emanuela Mazzone, and Russell Beale. 2009. Under my Pillow – Designing Security for Children's Special Things. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*. BCS Learning & Development Ltd. Swindon, UK, Cambridge, UK, 288–292. https://dl.acm.org/citation.cfm?id=1671046

[254] David Recordon and Drummond Reed. 2006. OpenID 2.0: A Platform for User-Centric Identity Management. In *Proceedings of the second ACM workshop on Digital identity management - DIM '06*. ACM Press, Alexandria, VA, USA, 11–15. DOI:http://dx.doi.org/10.1145/1179529.1179532

[255] Karen Renaud and Antonella De Angeli. 2009. Visual Passwords: Cure-All or Snake Oil? *Commun. ACM* 52, 12 (2009), 135–140. DOI:http://dx.doi.org/10.1145/1610252.1610287

[256] Karen Renaud and Verena Zimmermann. 2018. Nudging folks towards stronger password choices: providing certainty is the key. *Behavioural Public Policy* (feb 2018), 1–31. DOI:http://dx.doi.org/10.1017/bpp.2018.3

[257] Karen Renaud, Verena Zimmermann, Joseph Maguire, and Steve Draper. 2017. Lessons Learned from Evaluating Eight Password Nudges in the Wild. In *Proceedings of The {LASER} Workshop: Learning from Authoritative Security Experiment Results ({LASER} 2017)*. USENIX Association, Arlington, VA, USA, 25–37.

[258] Steve Riley. 2006a. It's Me, and Here's My Proof: Why Identity and Authentication Must Remain Distinct. (2006). https://technet.microsoft.com/en-us/library/cc512578.aspx

[259] Shannon Riley. 2006b. Password security: what users know and what they actually do. *Usability News* 8, 1 (2006), 2833–2836. http://dl.acm.org/citation.cfm?id=1240866.1241089

[260] Luis Roalter, Stefan Diewald, Andreas Möller, Tobias Stockinger, and Matthias Kranz. 2013. User-Friendly Authentication and Authorization Using a Smartphone Proxy. In *Computer Aided Systems Theory - EUROCAST 2013*. Springer Berlin Heidelberg, Las Palmas de Gran Canaria, Spain, 390–399. DOI:http://dx.doi.org/10.1007/978-3-642-53862-9_50

[261] Joel Ross, Lilly Irani, M Six Silberman, Andrew Zaldivar, and Bill Tomlinson. 2010. Who are the Crowdworkers ? Shifting Demographics in Mechanical Turk. *Chi 2010* JANUARY 2010 (2010), 2863–2872. DOI:http://dx.doi.org/10.1145/1753846.1753873

[262] Scott Ruoti, Brent Roberts, and Kent Seamons. 2015. Authentication Melee: A Usability Analysis of Seven Web Authentication Systems. In *Proceedings of the 24th International Conference on World Wide Web - WWW '15*. ACM Press, Geneva, Switzerland, 916–926. DOI:http://dx.doi.org/10.1145/2736277.2741683

[263] Richard M. Ryan and Edward L. Deci. 2000. Self-Determination Theory and the Facilitation of Intrinsic Motivation. *American Psychologist* 55, 1 (2000), 68–78. DOI:http://dx.doi.org/10.1037/0003-066X.55.1.68

[264] Marlies Rybnicek, Christoph Lang-Muhr, and Daniel Haslinger. 2014. A roadmap to continuous biometric authentication on mobile devices. In *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, Nicosia, Cyprus, 122–127. DOI:http://dx.doi.org/10.1109/IWCMC.2014.6906343

[265] Martina Angela Sasse. 2015. Scaring and Bullying People into Security Won't Work. *Security & Privacy Economics* May/June (2015), 80–83.

[266] Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. 2001. Transforming the "Weakest Link": A Human-Computer Interaction Approach for Usable and Effective Security. *BT Technology Journal* 19, 3 (2001), 122–131. DOI:http://dx.doi.org/10.1023/A:1011902718709

[267] Martina Angela Sasse and Ivan Flechais. 2005. Usable Security: Why Do We Need It? How Do We Get It? In *Security and Usability: Designing secure systems that people can use*, Lorrie Faith Cranor and Simson L. Garfinkel (Eds.). O'Reilly Media, Inc., Sebastopol, CA, USA, Chapter 2, 13–30. http://discovery.ucl.ac.uk/20345/

[268] M Angela Sasse, Matthew Smith, Cormac Herley, Heather Lipford, and Kami Vaniea. 2016. Debunking Security – Usability Tradeoff Myths. *IEEE Security and Privacy* 14, 5 (2016), 33–39.

[269] Florian Schaub, Ruben Deyhle, and Michael Weber. 2012. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia - MUM '12*. ACM Press, Ulm, Germany, 1. DOI:http://dx.doi.org/10.1145/2406367.2406384

[270] Roland Schlöglhofer and Johannes Sametinger. 2012. Secure and usable authentication on mobile devices. In *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia - MoMM '12*. ACM Press, Bali, Indonesia, 257–263. DOI:http://dx.doi.org/10.1145/2428955.2429004

[271] David Schmidt and Trent Jaeger. 2013. Pitfalls in the automated strengthening of passwords. In *Proceedings of the 29th Annual Computer Security Applications Conference on - ACSAC '13*. ACM, New Orleans, Lousiana, USA, 129–138. DOI:http://dx.doi.org/10.1145/2523649.2523651

[272] Bruce Schneier. 2006. Real-World Passwords - Schneier on Security. (2006). https://www.schneier.com/blog/archives/2006/12/realworld

[273] Bruce Schneier. 2013. The Psychology of Security. In *Proceedings of Progress in Cryptology – AFRICACRYPT 2008*, Serge Vaudenay (Ed.). Springer Berlin Heidelberg, Casablanca, Morocco, 50–79. DOI:http://dx.doi.org/10.1007/978-3-540-68164-9_5

[274] Sean M. Segreti, William Melicher, Saranga Komanduri, Darya Melicher, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L. Mazurek. 2017. Diversify to Survive: Making Passwords Stronger with Adaptive Policies. In *e Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, USA, 1–12. https://www.usenix.org/system/files/conference/soups2017/soups2017-segreti.pdf

[275] Tobias Seitz. 2016. *The Decoy Effect for Passwords - A First Exploration*. Technical Report. Ludwig-Maximilians-Universität München, Munich, Germany. 8 pages. DOI:http://dx.doi.org/10.13140/RG.2.1.2308.8880

[276] Tobias Seitz, Manuel Hartmann, Jakob Pfab, and Samuel Souque. 2017. Do Differences in Password Policies Prevent Password Reuse?. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '17*. ACM Press, New York, New York, USA, 2056–2063. DOI:http://dx.doi.org/10.1145/3027063.3053100

[277] Tobias Seitz and Heinrich Hussmann. 2017. PASDJO: Quantifying Password Strength Perceptions with an Online Game. In *Proceedings of the 29th Australian Conference on Human-Computer Interaction (OzCHI 2017)*. ACM, Brisbane, Australia, 9. DOI:http://dx.doi.org/10.1145/3152771.3152784

[278] Tobias Seitz, Emanuel von Zezschwitz, Stefanie Meitner, and Heinrich Hussmann. 2016. Influencing Self-Selected Passwords Through Suggestions and the Decoy Effect. In *Proceedings of the 1st European Workshop on Usable Security*. Internet Society, Darmstadt, 2:1–2:7. DOI:http://dx.doi.org/10.14722/eurousec.2016.23002

[279] C. E. Shannon. 1951. Prediction and Entropy of Printed English. *Bell System Technical Journal* 30, 1 (1951), 50–64. DOI:http://dx.doi.org/10.1002/j.1538-7305.1951.tb01366.x

[280] Richard Shay. 2015. *Creating Usable Policies for Stronger Passwords with MTurk*. Dissertation. Carnegie Mellon University.

[281] Richard Shay and Elisa Bertino. 2009. A Comprehensive Simulation Tool for the Analysis of Password Policies. *International Journal of Information Security* 8, 4 (2009), 275–289. DOI:http://dx.doi.org/10.1007/s10207-009-0084-3

[282] Richard Shay, Adam L Durity, Sean M Segreti, Blase Ur, Lujo Bauer, and Nicolas Christin. 2016. Designing Password Policies for Strength and Usability. *ACM Transactions on Information and System Security* 18, 4 (2016), 13:1–13:34. DOI:http://dx.doi.org/10.1145/2891411

[283] Richard Shay, Iulia Ion, Robert W Reeder, and Sunny Consolvo. 2014. "My religious aunt asked why i was trying to sell her viagra": Experiences with account hijacking. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*. ACM Press, Toronto, ON, Canada, 2657–2666. DOI:http://dx.doi.org/10.1145/2556288.2557330

[284] Richard Shay, Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Blase Ur, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2012. Correct Horse Battery Staple. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, Washington, DC, USA, 1–20. DOI:http://dx.doi.org/10.1145/2335356.2335366

[285] Richard Shay, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Nicolas Christin, and Lorrie Faith Cranor. 2010. Encountering Stronger Password Requirements : User Attitudes and Behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. ACM, Redmond, WA, USA, Article 2, 20 pages. DOI:http://dx.doi.org/10.1145/1837110.1837113

[286] Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip Seyoung Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2014. Can Long Passwords Be Secure and Usable. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*. ACM Press, Toronto, ON, Canada, 2927–2936. DOI:http://dx.doi.org/10.1145/2556288.2557377

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

In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2903–2912. DOI:http://dx.doi.org/10.1145/2702123.2702586

[288] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. 2010. Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *ACM Transactions on Internet Technology (TOIT)* 10, 2 (2010), 373 – 382. DOI:http://dx.doi.org/10.1145/1753326.1753383

[289] Michael Sherman, Gradeigh Clark, Yulong Yang, Shridatt Sugrim, Arttu Modig, Janne Lindqvist, Antti Oulasvirta, and Teemu Roos. 2014. User-generated free-form gestures for authentication. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services - MobiSys '14*. ACM Press, Bretton Woods, NH, USA, 176–189. DOI:http://dx.doi.org/10.1145/2594368.2594375

[290] M. Shevlin and J.N.V. Miles. 1998. Effects of sample size, model specification and factor loadings on the GFI in confirmatory factor analysis. *Personality and Individual Differences* 25 (1998), 85–90. DOI:http://dx.doi.org/10.1016/S0191-8869(98)00055-5

[291] Jordan Shropshire, Merrill Warkentin, Allen C. Johnston, and Mark B. Schmidt. 2006. Personality and IT security: An application of the five-factor model. *Americas Conference on Information Systems (AMCIS)* January (2006), 3443–3449.

[292] Jordan Shropshire, Merrill Warkentin, and Shwadhin Sharma. 2015. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security* 49 (2015), 177–191. DOI:http://dx.doi.org/10.1016/j.cose.2015.01.002

[293] Itamar Simonson. 1989. Choice Based on Reasons: The Case of Attraction and Compromise Effects. *Journal of Consumer Research* 16, 2 (1989), 158. DOI:http://dx.doi.org/10.1086/209205

[294] Supriya Singh, Anuja Cabraal, Catherine Demosthenus, Gunela Astbrink, and Michele Furlong. 2007. Password Sharing: Implications for Security Design Based on Social Practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, San Jose, CA, USA, 895–904. DOI:http://dx.doi.org/10.1145/1978942.1979324

[295] Andreas Sotirakopoulos, Kirstie Hawkey, and Konstantin Beznosov. 2011. On the challenges in usable security lab studies. In *Proceedings of the Seventh Symposium on Usable Privacy and Security - SOUPS '11*. ACM Press, Pittsburgh, PA, USA, 1. DOI:http://dx.doi.org/10.1145/2078827.2078831

[296] Sanjay Srivastava, Oliver P. John, Samuel D. Gosling, and Jeff Potter. 2003. Development of personality in early and middle adulthood: Set like plaster or persistent change? *Journal of Personality and Social Psychology* 84, 5 (2003), 1041–1053. DOI:http://dx.doi.org/10.1037/0022-3514.84.5.1041

[297] Clemens Stachl, Sven Hilbert, Jiew-Quay Au, Daniel Buschek, Alexander De Luca, Bernd Bischl, Heinrich Hussmann, and Markus Bühner. 2017. Personality Traits Predict Smartphone Usage. *European Journal of Personality* 31, 6 (nov 2017), 701–722. DOI:http://dx.doi.org/10.1002/per.2113

[298] Frank Stajano and Paul Wilson. 2011. Understanding Scam Victims: Seven Principles for Systems Security. *Commun. ACM* 54, 3 (2011), 70. DOI:http://dx.doi.org/10.1145/1897852.1897872

[299] Michelle Steves, Mary Theofanos, Celia Paulsen, and Athos Ribeiro. 2015. Password Policy Languages: Usable Translation from the Informal to the Formal. In *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS '15)*. Springer International Publishing, Los Angeles, CA, USA, 119–130. DOI:http://dx.doi.org/10.1007/978-3-319-20376-8_11

[300] Elizabeth Stobert. 2014. The Agony of Passwords: Can We Learn from User Coping Strategies?. In *Proceedings of the extended abstracts of the 32nd annual ACM conference on Human factors in computing systems - CHI EA '14*. ACM Press, Toronto, ON, Canada, 975–980. DOI:http://dx.doi.org/10.1145/2559206.2579421

[301] Elizabeth Stobert and Robert Biddle. 2013. Memory retrieval and graphical passwords. In *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*. ACM, Newcastle, UK, 1. DOI:http://dx.doi.org/10.1145/2501604.2501619

[302] Elizabeth Stobert and Robert Biddle. 2014a. A Password Manager that Doesn't Remember Passwords. In *Proceedings of the 2014 workshop on New Security Paradigms Workshop*. ACM, Victoria, BC, Canada, 39–52. DOI:http://dx.doi.org/10.1145/2683467.2683471

[303] Elizabeth Stobert and Robert Biddle. 2014b. The Password Life Cycle: User Behaviour in Managing Passwords. In *Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS '14)*. USENIX Association, Menlo Park, CA, USA, 243–255.

[304] Elizabeth Stobert and Robert Biddle. 2015. Expert Password Management. In *Proceedings of Passwords 2015*. Springer International Publishing, 3–20. https://passwordscon.org/wp-content/uploads/2015/05/preproceedings.pdf

[305] Elizabeth Ann Stobert. 2015. *Graphical Passwords and Practical Password Management*. Doctoral Thesis. Carlton University.

[306] Tobias Stockinger. 2011. *Implicit authentication for mobile devices*. Technical Report. Media Informatics Group, Munich, Germany.

[307] Tobias Stockinger, Marion Koelle, Patrick Lindemann, Matthias Kranz, and Luis Roalter. 2015. Towards Leveraging Behavioral Economics in Mobile Application Design. In *Gamification in Education and Business*, Torsten Reiners and Lincoln Woods (Eds.). Springer International Publishing, 105–131. DOI:http://dx.doi.org/10.1007/978-3-319-10208-5_6

[308] San-tsai Sun, Yazan Boshmaf, Kirstie Hawkey, and Konstantin Beznosov. 2010. A Billion Keys, but Few Locks: The Crisis of Web Single Sign-On. In *Proceedings of the 2010 workshop on New security paradigms - NSPW '10*. ACM, Concord, MA, USA, 61–72. DOI:http://dx.doi.org/10.1145/1900546.1900556

[309] San-tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. 2011. What makes users refuse web single sign-on? An Empirical Investigation of OpenID. In *Proceedings of the Seventh Symposium on Usable Privacy and Security - SOUPS '11*. ACM Press, Pittsburgh, PA, USA, 1–20. DOI:http://dx.doi.org/10.1145/2078827.2078833

[310] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. Crying Wolf: An Empirical Study of SSL Warning Effectivenes. In *18th USENIX Security Symposium*. USENIX Association, Montréal, Québec, Canada, 399–432. DOI:http://dx.doi.org/10.1016/S1353-4858(01)00916-3

[311] Michael Cheng Tek Tai. 2012. Deception and informed consent in social, behavioral, and educational research (SBER). *Tzu Chi Medical Journal* 24, 4 (2012), 218–222. DOI:http://dx.doi.org/10.1016/j.tcmj.2012.05.003

[312] Mohammad Tamviruzzaman, Sheikh Iqbal Ahamed, Chowdhury Sharif Hasan, and Casey O'brien. 2009. ePet: When Cellular Phone Learns to Recognize Its Owner. In *Proceedings of the 2nd ACM workshop on Assurable and usable security configuration - SafeConfig '09*. ACM Press, Chicago, IL, USA, 13–17. DOI:http://dx.doi.org/10.1145/1655062.1655066

[313] Andrew S. Tanenbaum and D. (David) Wetherall. 2011. *Computer networks* (5th editio ed.). Pearson Prentice Hall. 933 pages. https://books.google.de/books?id=2xWHAQAACAAJ

[314] Furkan Tari, A. Ant Ozok, and Stephen H. Holden. 2006. A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords. In *Proceedings of the second symposium on Usable privacy and security - SOUPS '06*. ACM Press, Pittsburgh, PA, USA, 56–66. DOI:http://dx.doi.org/10.1145/1143120.1143128

[315] RH Thaler. 2004. Mental accounting matters. Vol. 206. Princeton University Press, Chapter 3, 183–206. http://books.google.com/books?hl=en

[316] Richard H. Thaler. 1999. Mental Accounting Matters. *Journal of Behavioral Decision Making* 12, 3 (sep 1999), 183–206. DOI:http://dx.doi.org/10.1002/(SICI)1099-0771(199909)12:3<183::AID-BDM318>3.0.CO;2-F

[317] Richard H. Thaler and Cass R. Sunstein. 2008. *Nudge: Improving Decisions about Health, Wealth, and Happiness*. Yale University Press. https://books.google.com/books?hl=de

[318] Richard H Thaler, Cass R Sunstein, and John P Balz. 2010. Choice Architecture. *Social Science Research Network* April (2010). DOI:http://dx.doi.org/10.2139/ssrn.1583509

[319] Julie Thorpe, Muath Al-Badawi, Brent MacRae, and Amirali Salehi-Abari. 2014. The presentation effect on graphical passwords. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*. ACM Press, Toronto, ON, Canada, 2947–2950. DOI:http://dx.doi.org/10.1145/2556288.2557212

[320] Noam Tractinsky. 1997. Aesthetics and apparent usability: empirically assessing cultural and methodological issues. *Proceedings of the ACM SIGCHI Conference on ...* (1997), 115–122. http://dl.acm.org/citation.cfm?id=258626

[321] Noam Tractinsky, Adi Katz, and D. Ikar. 2000. What is beautiful is usable. *Interacting with Computers* 13, 2 (2000), 127–145. DOI:http://dx.doi.org/10.1016/S0953-5438(00)00031-X

[322] Harshal Tupsamudre, Vijayanand Banahatti, and Sachin Lodha. 2016. POSTER : Improved Markov Strength Meters for Passwords. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. ACM, Vienna, Austria. DOI:http://dx.doi.org/10.1145/2976749.2989058

[323] Amos Tversky and Daniel Kahneman. 1974. Judgment under Uncertainty: Heuristics and Biases. *Science* 185, 4157 (sep 1974), 1124–31. DOI:http://dx.doi.org/10.1126/science.185.4157.1124

[324] Sven Uebelacker and Susanne Quiel. 2014. The Social Engineering Personality Framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust*. IEEE, Vienna, Austria, 24–30. DOI:http://dx.doi.org/10.1109/STAST.2014.12

[325] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. 2013. Quantifying the security of graphical passwords: the case of android unlock patterns. *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13* 44, 4 (2013), 161–172. DOI:http://dx.doi.org/10.1145/2508859.2516700

[326] Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, Noah Johnson, and William Melicher. 2017. Design and Evaluation of a Data-Driven Password Meter. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, Denver, CO, USA, 3775–3786. DOI:http://dx.doi.org/10.1145/3025453.3026050

[327] Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Do Users' Perceptions of Password Security Match Reality ?. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, San Jose, CA, USA, 3748–3760. DOI:http://dx.doi.org/10.1145/2858036.2858546

[328] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2012a. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *Proceedings of the 21st USENIX Security symposium*. USENIX Association, Bellevue, WA, USA, 5–16. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final209.pdf

[329] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Julio López. 2012b. Helping Users Create Better Passwords. *;login* 37, 6 (2012), 51–57. http://scholar.google.co.uk/scholar?q=the+science+of+guessing+bonneau

[330] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015a. "I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '15)*. USENIX Association, Ottawa, Canada, 123–140.

[331] Blase Ur, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Saranga Komanduri, Darya Kurilova, Michelle L Mazurek, William Melicher, and Richard Shay. 2015b. Measuring Real-World Accuracies and Biases in Modeling Password Guessability. In *24th USENIX Security Symposium (USENIX Security 15)*. USENIX Association, Washington, DC, USA, 463—-481. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/ur

[332] Anthony Vance, David Eargle, Kirk Ouimet, and Detmar Straub. 2013. Enhancing password security through interactive fear appeals: A web-based field experiment. In *Proceedings of the*

Annual Hawaii International Conference on System Sciences (HICSS'13). IEEE, Koloa, HI, USA, 2988–2997. DOI:http://dx.doi.org/10.1109/HICSS.2013.196

[333] Rafael Veras, Christopher Collins, and Julie Thorpe. 2014. On the Semantic Patterns of Passwords and their Security Impact. In *Proceedings 2014 Network and Distributed System Security Symposium*. Internet Society, Reston, VA, USA, 23–26. DOI:http://dx.doi.org/10.14722/ndss.2014.23103

[334] Rafael Veras, Julie Thorpe, and Christopher Collins. 2012. Visualizing semantics in passwords. In *Proceedings of the Ninth International Symposium on Visualization for Cyber Security - VizSec '12*. ACM Press, Seattle, WA, USA, 88–95. DOI:http://dx.doi.org/10.1145/2379690.2379702

[335] Vilhelm Verendel. 2008. *A Prospect Theory approach to Security*. Technical Report 08. Göteborg University, Göteborg.

[336] George E Violettas and Kyriakos Papadopoulos. 2014. Passwords to absolutely avoid (A Survey in Greece). In *The Fifth International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2014)*. IEEE, Bangalore, India, 60–68. DOI:http://dx.doi.org/10.1109/ICADIWT.2014.6814693

[337] Melanie Volkamer and Karen Renaud. 2013. Mental Models – General Introduction and Review of Their Application to Human-Centred Security. Vol. 8260. Springer Berlin Heidelberg, 255–280. DOI:http://dx.doi.org/10.1007/978-3-642-42001-6_18

[338] Emanuel Von Zezschwitz. 2016. *Risks and Potentials of Graphical and Gesture-based Authentication for Touchscreen Mobile Devices*. PhD Thesis. Ludwig-Maximilians Universität München.

[339] Emanuel Von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2013. Survival of the shortest: A retrospective analysis of influencing factors on password composition. In *Human-Computer Interaction – INTERACT 2013, Lecture Notes in Computer Science*, Paula Kotzé, Gary Marsden, Gitte Lindgaard, Janet Wesson, and Marco Winckler (Eds.). Vol. 8119. Springer Berlin Heidelberg, 460–467. DOI:http://dx.doi.org/10.1007/978-3-642-40477-1_28

[340] Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2014. Honey, I Shrunk the Keys: Influences of Mobile Devices on Password Composition and Authentication Performance. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction Fun, Fast, Foundational - NordiCHI '14*. ACM Press, Helsinki, Finland, 461–470. DOI:http://dx.doi.org/10.1145/2639189.2639218

[341] Emanuel von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. 2015. Easy to Draw, but Hard to Trace? On the Observability of Grid-based (Un)lock Patterns. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*. ACM Press, Seoul, South Korea, 2339–2342. DOI:http://dx.doi.org/10.1145/2702123.2702202

[342] Emanuel von Zezschwitz, Malin Eiband, Daniel Buschek, Sascha Oberhuber, Alexander De Luca, Florian Alt, and Heinrich Hussmann. 2016. On quantifying the effective password space of grid-based unlock gestures. In *Proceedings of the 15th International Conference on Mobile and Ubiquitous Multimedia - MUM '16*. ACM Press, Rovaniemi, Finland, 201–212. DOI:http://dx.doi.org/10.1145/3012709.3012729

[343] Ding Wang. 2016. Targeted Online Password Guessing: An Underestimated Threat. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. ACM, Vienna, Austria, 1242–1254. DOI:http://dx.doi.org/10.1145/2976749.2978339

[344] Ding Wang, Haibo Cheng, and Ping Wang. 2015. *Understanding Passwords of Chinese Users : Characteristics , Security and Implications*. Technical Report.

[345] Ding Wang, Debiao He, Haibo Cheng, and Ping Wang. 2016. fuzzyPSM: A New Password Strength Meter Using Fuzzy Probabilistic Context-Free Grammars. In *Proceedings of the International Conference on Dependable Systems and Networks (DSN)*. IEEE, 595–606. DOI:http://dx.doi.org/10.1109/DSN.2016.60

[346] Ding Wang and Ping Wang. 2015. The Emperor's New Password Creation Policies. In *Proceedings of the 20th European Symposium on research in Computer Security - ESORICS'15*. Springer, Vienna, Austria, 456–477. DOI:http://dx.doi.org/10.1007/978-3-319-24177-7

[347] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*. ACM Press, Redmond, WA, USA, 1. DOI:http://dx.doi.org/10.1145/1837110.1837125

[348] Rick Wash, Emilee Rader, Ruthie Berman, Macalester College, Rick Wash, Emilee Rader, and Ruthie Berman. 2016. Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites. In *Symposium on Usable Privacy and Security - SOUPS'16*. USENIX Association, Denver, CO, USA, 175–188.

[349] Rick Wash, Emilee Rader, and Chris Fennell. 2017. Can People Self-Report Security Accurately? Agreement Between Self-Report and Behavioral Measures. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. ACM Press, Denver, CO, USA, 2228–2232. DOI:http://dx.doi.org/10.1145/3025453.3025911

[350] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. 2010. Testing metrics for password creation policies by attacking large sets of revealed passwords. *Proceedings of the 17th ACM conference on Computer and communications security - CCS '10* (2010), 162. DOI:http://dx.doi.org/10.1145/1866307.1866327

[351] Matt Weir, Sudhir Aggarwal, Breno de Medeiros, and Bill Glodek. 2009. Password Cracking Using Probabilistic Context-Free Grammars. In *2009 30th IEEE Symposium on Security and Privacy*. IEEE, Oakland, CA, USA, 391–405. DOI:http://dx.doi.org/10.1109/SP.2009.8

[352] Dirk Weirich and Martina Angela Sasse. 2001a. Persuasive Password Security. In *CHI '01 extended abstracts on Human factors in computing systems - CHI '01*. ACM Press, Minneapolis, Minnesota, USA, 139–140. DOI:http://dx.doi.org/10.1145/634067.634152

[353] Dirk Weirich and Martina Angela Sasse. 2001b. Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World. In *Proceedings of the 2001 Workshop on New Security Paradigms (NSPW '01)*. ACM, Cloudcroft, NM, USA, 137–143. DOI:http://dx.doi.org/10.1145/634149.634152

[354] Daniel Lowe Wheeler. 2016. zxcvbn: Low-Budget Password Strength Estimation. In *Proceedings of the 25th USENIX Security Symposium (USENIX Security 16)*. USENIX Association, Austin, TX, 157–173. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/wheeler

[355] Andrew M White, Katherine Shaw, Fabian Monrose, and Elliott Moreton. 2014. Isn't that Fantabulous: Security, Linguistic and Usability Challenges of Pronounceable Tokens. In *Proceedings of the 2014 workshop on New Security Paradigms Workshop - NSPW '14*. ACM Press, Victoria, British Columbia, Canada, 25–38. DOI:http://dx.doi.org/10.1145/2683467.2683470

[356] Alma Whitten and J. D. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium*. USENIX Association, Washington, DC, USA, 169–184. DOI:http://dx.doi.org/169-184

[357] Susan Wiedenbeck, Jim Waters, Jean Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human Computer Studies* 63, 1-2 (2005), 102–127. DOI:http://dx.doi.org/10.1016/j.ijhcs.2005.04.010

[358] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. 2006. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the working conference on Advanced visual interfaces - AVI '06*. ACM Press, Venezia, Italiy, 177. DOI:http://dx.doi.org/10.1145/1133265.1133303

[359] Craig Wiggington, Mike Curran, and Terrence Karner. 2017. *2017 Global Mobile Consumer Survey: US Edition*. Technical Report. Deloitte. 1–29 pages. http://www2.deloitte.com/be/en.html

[360] Daricia Wilkinson, Saadhika Sivakumar, David Cherry, Bart P Knijnenburg, Elaine M Raybourn, Pamela Wisniewski, and Henry Sloan. 2017. (Work in Progress) User-Tailored Privacy by Design. In *Proceedings of USEC'17*. Internet Society, 1–12.

[361] Naomi Woods and Mikko Siponen. 2018. Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human-Computer Studies* 111, Supplement C (2018), 36–48. DOI:http://dx.doi.org/https://doi.org/10.1016/j.ijhcs.2017.11.002

[362] Min Wu, Robert C. Miller, and Simson L. Garfinkel. 2006. Do Security Toolbars Actually Prevent Phishing Attacks?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*. ACM, Montréal, Québec, Canada, 601–610. DOI:http://dx.doi.org/10.1145/1124772.1124863

[363] Heng Xu, Mb Rosson, and Jm Carroll. 2007. Increasing the Persuasiveness of IT Security Communication: Effects of Fear Appeals and Self-View. In *Workshop on Usable IT Security Management, Symposium on Usable Privacy and Security (SOUPS)*. Carnegie Mellon University, Pittsburgh, PA, USA, 1–4. http://cups.cs.cmu.edu/soups/2007/workshop/IT

[364] Jeff Yan, Blackwell Alan, Ross Anderson, and Alasdair Grant. 2004. Password Memorability and Security: Empirical Results. *IEEE Security and Privacy* 2, 5 (2004), 25–31. DOI:http://dx.doi.org/10.1109/MSP.2004.81

[365] Weining Yang, Ninghui Li, Omar Chowdhury, Aiping Xiong, and Robert W Proctor. 2016. An Empirical Study of Mnemonic Sentence-based Password Generation Strategies. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*. ACM Press, New York, New York, USA, 1216–1229. DOI:http://dx.doi.org/10.1145/2976749.2978346

[366] Yulong Yang, Janne Lindqvist, and Antti Oulasvirta. 2014. Text Entry Method Affects Password Security. In *Proceedings of the Learning from Authoritative Security Experiment Results Workshop (LASER '14)*. USENIX Association, Arlington, VA, USA, 11–20. https://www.usenix.org/system/files/conference/laser2014/laser-2014-paper-yang.pdf

[367] Zishuang (Eileen) Ye, Sean Smith, and Denise Anthony. 2005. Trusted Paths for Browsers. *ACM Transactions on Information and System Security* 8, 2 (2005), 153–186. DOI:http://dx.doi.org/10.1145/1065545.1065546

[368] Ka-Ping Yee and Kragen Sitaker. 2006. Passpet: Convenient Password Management and Phishing Protection. In *Proceedings of the second symposium on Usable privacy and security - SOUPS '06*. ACM Press, Pittsburgh, PA, USA, 32–43. DOI:http://dx.doi.org/10.1145/1143120.1143126

[369] Indi Young. 2008. *Mental Models: Aligning Design Strategy with Human Behavior*. 299 pages. http://books.google.com/books?id=b5aLQ

[370] Wu Youyou, Michal Kosinski, and David Stillwell. 2015. Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences* 112, 4 (jan 2015), 1036–1040. DOI:http://dx.doi.org/10.1073/pnas.1418680112

[371] Nur Haryani Zakaria and Norliza Katuk. 2013. Towards designing effective security messages: Persuasive password guidelines. In *Proceedings of the International Conference on Research and Innovation in Information Systems (ICRIIS)*. IEEE, Kajang, Malaysia, 129–134. DOI:http://dx.doi.org/10.1109/ICRIIS.2013.6716697

[372] Yinqian Zhang, Fabian Monrose, and Michael K Reiter. 2010. The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis. In *Proceedings of the 17th ACM conference on Computer and communications security - CCS '10*. ACM Press, Chicago, IL, USA, 176. DOI:http://dx.doi.org/10.1145/1866307.1866328

[373] Leah Zhang-Kennedy, Sonia Chiasson, and Paul van Oorschot. 2016. Revisiting password rules: facilitating human management of passwords. In *Proceedings of the Symposium on Electronic Crime Research (eCrime)*. IEEE, Toronto, ON, Canada, 1–10. DOI:http://dx.doi.org/10.1109/ECRIME.2016.7487945