6
Password Policies and Reuse

In the previous chapter, we reached the conclusion that users' mental models of password strength are fairly accurate with small exceptions. We can thus expect that users at least try to create strong passwords if they deem the account worth protecting. However, this is only one side of the medal: password reuse is rampant. Coping with the high number of passwords by reusing them is common, but hard to defend against - in part because some degree of reuse is necessary [117, 385]. At the same time, password reuse might expose users to an even greater risk than weak passwords. Password reuse renders the security advantages of picking a very strong password void. In case an attacker obtains a user's plain text password, they gain access to all accounts that share this strong password. Studies have shown that users tend to underestimate the risks generated by password reuse **@ref**.

As explained in Section 3.3.1, password composition policies are one of the interventions targeted at weak passwords. However, in many cases users fulfill requirements in predictable ways; the primary goal is thus missed. So, if password policies do not always help password strength, they might still prevent password reuse: if they were heterogeneous across different web sites with mutually exclusive requirements, users cannot reuse passwords like they would naturally do. In this chapter, we investigate password policies of one hundred of the most-visited web-services in Germany and try to find how well their differences prevent password reuse. Some results of this investigation have been previously published together with Manuel Hartman, Jakob Pfab, and Samuel Souque [283]. In this chapter we shed light on the findings and discuss them in the context of supporting password authentication.

6.1 Background and Context

Password reuse is a major threat because it is easy for attackers to compromise many accounts at once. Even if users try to slightly modify their base password, attackers are still able to crack a large portion of the resulting passwords [68, 176]. There is mixed evidence about the subset of passwords that are reused more often, but generally one can identify a "go-to password" for regular sites, "high-value passwords" for important sites, and a "don't care" password for the rest [18, 312, 155, 112, 313, 341, 359].

Password policies were originally designed to combat weak passwords, but some of them try to steer users away from reused passwords. Usually, this is done through black lists that block passwords

that have already been exposed after a data breach. If a user tried to reuse a password which has been leaked, the system can detect this and enforce the creation of a new one. However, Habib et al. showed that users perform predictable alterations to circumvent the black-list filter [147]. In total, they identified 13 modification techniques. For instance, participants in the study added digits, symbols, words or letters. Habib et al. conclude that blacklists are thus only useful, if a user's second attempt does not obviously reuse the blacklisted word. Segreti et al. evaluated a different approach to combat reuse, known as the "Popularity is Everything" system [280]. Here, a password becomes blacklisted after a certain number of users have used the same password. Reuse in this case means reused by many users, instead of a single individual reusing the credentials multiple times.

In most cases, it is impossible to display the full list of blacklisted words in the user interface. Thus, to find out a site's policy, it has to be reverse engineered by testing different passwords and look if they are acceptable or not. Florêncio and Herley audited policies of public institutions and high-traffic website [113]. They found that online retailers have much looser password policies than government or university sites. Wang and Wang similarly checked the policies of 50 representative websites [357]. They took passwords from leaked datasets and picked 16 passwords with varying hypothetical strength. They did not aim to identify black-lists or special forbidden character types. Carnavalet and Mannan managed to automate dictionary checks by leveraging keep-alive connections [49]. However, they focused on server-side strength estimations rather than blacklists per se. To conduct research on policies in the wild, it would be favorable to have a repository that contains all policies. Steves et al. proposed to do crowd-source the data and define a formal language (based on XML) to describe policies [308]. The idea was later picked up and extended by Horsch et al. [167]. The repository would also be useful for a password generator that takes the site's policy into account to avoid rejected passwords. On the other hand, adversaries benefit from the policy repository, too. They could optimize guessing attacks by removing unnecessary guesses.

In summary, a password policy would ensure users pick adequately strong passwords and at the same time prevent dangerous reuse. Estimating the risk is still an open challenge. As of now, there have not been investigations into the efficacy to prevent reuse among current in-the-wild policies. Finding out whether current policies were suitable to combat password reuse as a whole was our primary objective.

6.2 Method

Studying password policies needs to address two central aspects: selecting representative web sites and selecting appropriate passwords. The first part is relatively straight-forward. We took Alexa.com rankings as indicator for the popularity of a website. To accomplish the analysis in a reasonable time frame, we took 100 web sites (100% more than Wang and Wang, and 33% more than Florêncio and Herley). In May 2016, ~~from the 100 most visited web sites in Germany,~~ 83 allowed public online registrations. The remaining 17 sites were banks, mobile carriers, or pay-tv providers who require offline registration and verification as a security measure. The websites and their policies are listed in Table 14.1 (Appendix). Although we took the most-visited websites in Germany, the results have implications for an international audience, because many of the audited sites operate globally.

The second challenge is finding suitable passwords to reverse-engineer password requirements. We approached this task in two separate stages to find a good candidate set.

First Stage: Identification of suitable passwords

Similar to Wang and Wang, we crafted 15 passwords showing typical password characteristics. The passwords followed common policy categories as proposed by Shay et al. [290]. For instance, some passwords met a *3class12* policy by including three different character classes (lower-/uppercase letters, digits) and a minimum length of 12. Next, we tried to register new accounts with all of these 15 passwords at all 83 websites. In case the site rejected the password, we investigated the reasons and modified the password until the policy was fulfilled. This new password was then added to our test set. During this stage, a number of sites revealed blacklisted symbols. If this was the case, we intentionally crafted a password with the blacklisted characters and added it to our set, so that we could se if other websites implicitly utilize the same blacklist. Similarly, if there were maximum length enforcements, we added a password longer than that to our list. This process resulted in a test set of **46** diverse passwords@**TODO** put in appendix. The list was structured by the following criteria:

length	minimum and maximum length restrictions
character classes	the presence of enforced character classes, i.e. mandatory, forbidden, and allowed characters
complexity	the most stringent policy that the password would fulfill, as classified by Shay et al. [290]. The categories were *basic*, *2class*, *3class*, and *complex*
dictionary	the presence of a pro-active dictionary check, including common passwords.
additional requirements	black-/whitelisted symbols instead of a whole character class, additional requirements like large enough edit-distance from username

Second Stage: Re-Evaluation with Extended Test Set

After identifying suitable passwords, we tried to use all of them on each web site, i.e. we performed a total of $46 * 83 = 3813$ checks. To avoid re-creating accounts with different email addresses, we tried to reset passwords wherever this was offered. Furthermore, we include top-level domains in the analysis that implement an Single-Sign On (SSO) scheme (e.g. live.com, msn.com, microsoft.com), because this might not be evident for the users.

6.3 Results

We found it was possible to create passwords that would meet 82 of the 83 policies (~98.88%). In the following we illustrate why this is possible.

6.3.1 Complexity

Most policies fell into the "basic" category. This means that their sole requirement was a minimum (or maximum) length. As shown in Figure 6.1, around three quarters of the sites used a basic policy[1]. Eleven web sites (13.3%) specifically require at least two different character types (*2class*). However, Ikea requires letters and digits, but would not count a symbol towards the two character classes. We

[1] In the CHI publication, we reported slightly different numbers: 57 *basic*, 11 *2class*, 3 *3class*, 1 *complex*, 10 *other*. It is in fact possible to put the *other* policies in the remaining found categories, which explains the updated distribution

still opted to categorize this as a *2class* policy (see remark in footnote 1). *Complex* policies in the wild have further restrictions, e.g. dictionary checks or special rules. 23 websites (27.7%) used a dictionary check. Bahn.de demanded three *different* characters, i.e. a password like `annnna` would be rejected, but `banana` would not. Paypal.com disallowed using the same character three times in a row, which rejects a couple of German compounds like `Schifffahrt`. Nevertheless, it is easy to find a password that fulfills the complexity requirements of all 83 websites: "D.ssertation18" is a 4class password that would pass all complexity requirements.

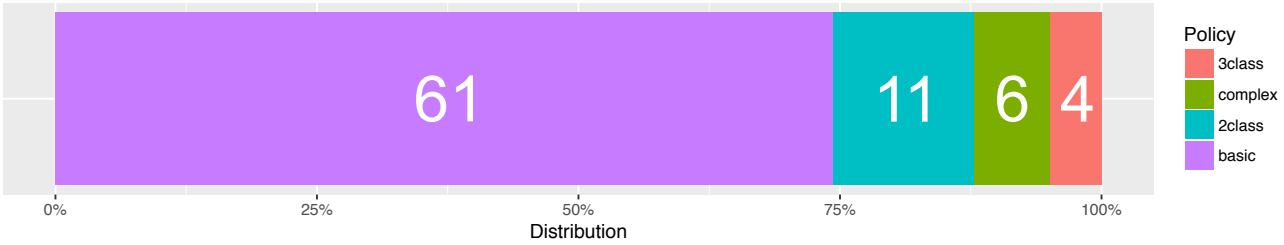

Figure 6.1: Distribution of minimum complexity of the policies. Most sites only require a given length.

Length requirements

The length requirements and restrictions were fairly inconsistent in the test set. The average minimum required length was $M = 6.3$ ($SD = 1.9$, see Figure 6.2). No website had a minimum length greater than nine characters. Among the top 10 most-visited sites, facebook.com, amazon.de, ebay.de allowed six-character passwords. Even system-generated 6-character passwords can be brute-forced in a matter of hours in an offline attack [2]. Wikipedia, which is also in the top 10, had a minimum length of one character. Interestingly, two tech-oriented websites allowed the same (heise.de and chip.de). Perhaps the service providers expect their technical audience to create stronger passwords anyhow, and they do also not much personal information. We were surprised that 40 sites (48.2%) imposed a *maximum* length restriction, which is counterproductive in terms of password security. The average maximum length was $M = 43$ characters ($SD = 32$). Ten websites rejected passwords longer than 20 characters, so a number of passphrases would be excluded.

In order to effectively prevent password re-use, the maximum length on one site would need to be lower than the minimum length of another site. This was not the case in any permutation of policy pairs. The closest difference was the maximum length at ikea.de (10 characters) and the minimum length at yahoo.com (9 characters). Thus, only a nine or ten character password could be reused on all the tested websites.

Character Sets

Although the websites at the top of the table, i.e. Google, Facebook, Amazon, all use a *basic* policy, there is still a high chance that they reject passwords containing certain characters. We found it was common to disallow non-ASCII symbols (see Table 6.1). For instance, Google rejected any passwords with non-ASCII characters. So, even dictionary words that include letters from non-English alphabets, e.g. the German umlauts ä,ö, and ü, will be rejected in this case. Some sites already provide a list of characters that are either allowed or disallowed at registration time. In the case of mobile.de, the list

[2] https://arstechnica.com/information-technology/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/ *(last accessed 27.01.2018)*

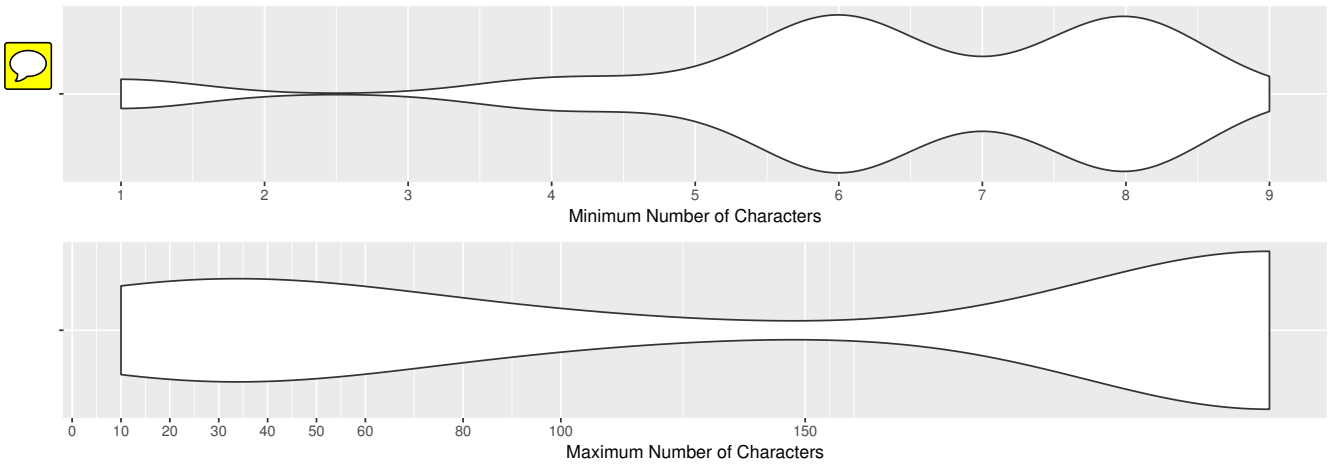

Figure 6.2: Density distribution of password length rules. We excluded maximum lengths beyond 245 characters, which explains the hard cut-off in the bottom plot.

of allowed symbols is even smaller. On the positive side of the spectrum, twitter.com accepted even extended Unicode characters like emojis.

A few websites did not reveal the list of allowed non-ASCII characters; some of our passwords were blocked if they contained certain characters. Thus, we had to remove character by character to find out which of them was blacklisted. For regular users, this process would be exceptionally tedious if their password contained a character from an unknown blacklist. Our audit shows that spaces and the tilde character '~' are the most likely culprits in this situation, which was the case at netflix.com, spiegel.de or welt.de. Finally, there were mutually exclusive policies: Lidl.de proactively shows a list of symbols from which the user has to choose at least one to create an account. However, all those symbols were disallowed on at least one other website. In that sense, in the unlikely case that a user's main password is accepted at lidl.de, chances are that it is rejected at a couple of other websites.

6.4 Discussion and Implications

In the following we shed light on what the results mean in terms of password reuse.

6.4.1 Policies are Mostly Homogenous

Overall we can state that in-the-wild policies are largely similar. The devil, however, lies in the details. It is not quite clear why almost half the websites enforce a maximum length restriction, albeit a high one in most cases. Shorter passwords are easier to guess in an offline attack. It is therefore almost necessary to lock out users after a number of failed login attempts to at least mitigate targeted online-guessing (see Section 2.2). Blocking non-ASCII characters further impedes users' password selection. Although the reasons for doing so are anything but obvious – allowing more characters increases the theoretical password space and thus potentially security, we interpret this restriction as a usability precaution. ASCII characters are part of virtually all physical keyboard layouts, but extended alphabets are not. For instance, if a German user's email password were "`DieÄrzte123`", they would be troubled to log into their account from a PC while abroad, because the umlauts are missing on the keyboard. Of course, there are ways to enter such characters, but they require much more effort under

Web site	Whitelisted symbols	Blacklisted symbols
ebay.de	!@#$%^*-_+=	
web.de	!#$%&()*+,-./:;<=>?@[\]^_{|}~§ÄäÖöÜüß	
gmx.net	!#$%&()*+,-./:;<=>?@[\]^_{|}~§ÄäÖöÜüß	
t-online.de	!#$%&()*+,-./<=>?@[\]_{|}~	
live.com	@#$%^*-_+=	
mobile.de	!$%&?-_+#	
pornhub.com	/_	
1und1.de	@#$%^*-_+=	
chefkoch.de	äöüÄÖÜß, _, -, !?&.	
zeit.de	äöüÄÖÜß ,.!?:;#&* ()_+=/<>-	
lidl.de	@#$%^&+=.:-!?	
spiegel.de		‘space’ ‘new line’
outbrain.com		‘space’
welt.de		‘space’
netflix.com		~

Table 6.1: Many websites only allow ASCII characters. This table shows the sites that restrict the ASCII set even further. Some sites are mutually exclusive regarding the usage of certain symbols only by looking at a small subset of the tested sites, e.g. netflix.com and t-online.de. The full rules can be found in the Appendix 14.1

these circumstances. The user experience of the entire login process would suffer, which is the reason for blocking the characters in the first place. However, with the increasing number of personal mobile devices that also work abroad, the motivation to block non-ASCII characters crumbles. Artificially blocking non-alphanumeric ASCII symbols, like $ or ;, in any case creates unnecessary burden for users. As we have seen in the previous Chapter, users attribute password strength to such symbols and forbidding them can lead to confusion and erroneous mental models. Perhaps the restriction was introduced to prevent site vulnerabilities, e.g. SQL injections. But this is a premier example for a misguided security approach that shifts effort to millions of users rather than to a couple of security engineers.

6.4.2 Policies do not prevent password-reuse

Neither length, nor complexity requirements were heterogeneous enough to prevent password reuse. In the end, only artificial character-class restrictions narrowed down the list of passwords that can be used everywhere. We found that a nine or ten character password, that includes at least one uppercase letter, one lowercase letter, and one digit would have been accepted by 82 of the 83 tested web sites. To circumvent dictionary checks, it is recommendable to intersperse digits in the middle. Thus, if users pick a password like `s1lverPWD`, current in-the-wild policies do not stand in their way. With an edit distance of 1, many rejected passwords can be turned into an accepted password if the rejection was caused by a special character. However, the criteria for the most-reusable password (we can call it the “golden password”) are very well-defined and narrow. Any password that does not meet these criteria will generate usability issues for users, e.g. if they use longer passwords or ones with a richer character set. Password generation is hampered in many cases by length limitations. In that sense, policies help to prevent re-use of passwords that could be considered either exceptionally weak, or stronger than average. Reuse of “normal” passwords that work everywhere is not prevented.

As a consequence, a policy could be adjusted dynamically if the users signs up with a “golden password”. It is very likely that a password showing the above described characteristics is reused

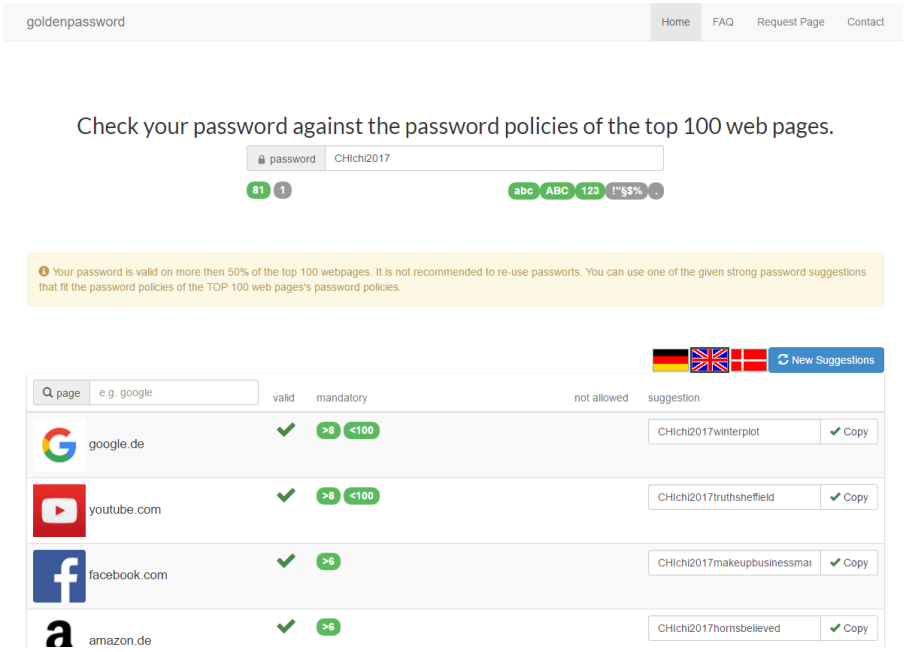

Figure 6.3: We built a small web app to demonstrate how contextual policy information can be used to a) generate suitable passwords and b) find out which web sites accept a given password.

across many web sites. As Florêncio et al. pointed out, this is not necessarily a bad thing [117]. However, if a high-value password is reused for an unimportant account, this interference could lead to problems. Stobert showed that experts are less prone to this threat [313], but regular users cannot always estimate the importance of an account up front. As a consequence, dynamically adjusting the policy could be a solution. Alternatively, it might be feasible to more prominently warn users about reuse and explain the implications. As shown by Ur et al., showing alternatives can help in this situation.

6.4.3 Smarter Password Generation

Our data clearly shows that generating random passwords can become troublesome for users: many policies restrict the length and allowed characters. Although many password generators allow the users to adjust some parameters of password creation (like Apple's system shown in Figure 3.4), more effort is required to find the right parameters. Thus, a system designed to take away cognitive effort becomes effortful once more. A better solution is to use contextual information for password generation. Typically, password managers have built-in generators. To avoid that users have to adjust parameters, a password manager could automatically retrieve the policy for a given website (context) and generate a strong password that fulfills it. As a proof of concept, we built a web-based prototype that demonstrates how contextual policy information can be used for password generation[3] (see Figure 6.3).

6.4.4 Limitations

Although the data can be very useful for password generators and for the design of future composition policies, it is limited in some ways. First, the list of web sites is not comprehensive, we merely observed a tiny snapshot of the high-traffic websites, which already required days of work for the entire

[3] http://jakob-p.github.io/goldenpassword/ *(last accessed 26.01.2018)*

team. We also could have investigated the top websites in different categories to get an even more representative sample. However, the current dataset already depicts the state of affairs in reasonable detail, and is comparable to similar publications [113, 357]. Furthermore, the longest password in our test set had a length of 246 characters. We concluded that there is no length restriction if this password was accepted by a given website, but there might just be a higher restriction. Nevertheless, since only a fraction of users use passwords this long, this limitation has almost no consequences.

Moreover, for several reasons we did not include emojis in all our tests although they are in fact part of the unicode character set. First, emojis break some input fields, because most of them are encoded with 4 bytes instead of 2. This means that they show up as two characters in the input field, which distorts length requirements. Furthermore, not all websites were encoded in the extended UTF32 standard and hence failed to submit the data.

Lastly, password policies change over time. Since carrying out our research in May 2016, we found by randomly re-sampling policies that they have changed. For instance, idealo.de used to enforce a *complex* policy, but they have switched to a *basic6* as of January 2018. Therefore, our data has a limited lifespan. The big players on the list, like Facebook, Google, or Amazon, are slower to enforce new polices due to the even larger user base and business impact. An automated process similar to the one from Carnavalet and Mannan [49] could help validate the data in the future.

6.5 Conclusion and Future Work

In this project, we extensively audited password policies of the top 100 web sites in Germany. The data set is published for further analysis on GitHub[4]. 83 of the websites offered public registration, and we could reuse a single password on 82 of them. Hence, we were able to answer our main research question "*Do password policies prevent password reuse?*" with a resounding "**no**". Thus, we further question the use of strict password policies as a means to influence password selection. It has been shown that they do not necessarily lead to stronger passwords. Now we have shown that they also do not prevent reuse. As a consequence, it would be easier for users if restrictions on password selection were loosened. Restrictions enforcing a maximum length or a certain set of symbols should be abolished to ensure universal password generators integrate with the websites. A *basic8* policy appears to work for the major players, so more service providers can follow them. To account for the potential security vulnerabilities, blacklisted common passwords and adaptive blacklists are promising solutions [147, 280]. Future research should thus evaluate the specific blacklists and user support to help them find alternatives in case their password was blacklisted.

[4] https://github.com/mimuc/password-policy-dataset *(last accessed 25.01.2018)*

Take Aways

- Most password policies in the wild used a basic policy with length as the only requirement.
- About half of the policies enforced a maximum length.
- It was possible to reuse a nine or ten character password that includes uppercase and lowercase letters, and at least one digit on 98% of websites in the test set.
- Only the requirement of certain symbols generated conflicts between policies.
- The above characteristics also tell us that any user with a different selection strategy faces a usability backlash. Acting more securely by generating passwords automatically is hampered because some policies reject such passwords.

Glossary

ASCII American Standard Code for Information Interchange. 201

CHI ACM CHI Conference on Human Factors in Computing Systems. Largest venue of research in Human-Computer Interaction. 201

CMU Carnegie Mellon University (Pittsburgh, Pennsylvania, USA). 42, 201

ESM Experience Sampling Method. 43, 201

GAM generalized additive model. 107, 115, 201

HCI Human-Computer Interaction. 41, 42, 44, 201

HIT Human Intelligence Task. 42, 201

IRB Institutional Review Board. 39, 42, 201

LUDS lowercase, uppercase, digits, symbols. 51, 201

mTurk Amazon Mechanical Turk. Crowd-Sourcing platforms where workers ("turkers") complete micro tasks and receive a small payment.. 42, 65, 66, 70, 80, 175, 201

NIST National Institute of Standards and Technology.. 10, 18, 19, 21, 51, 54, 61, 201

PAF Persuasive Authentication Framework. 62–64, 78, 201

PANAS Positive Affect and Negative Affect Scale. 42, 201

password manager Password Manager. Software that supports a user in the task of managing credentials. Can be standalone or built into web browsers. Famous examples for standalone password managers: LastPass, 1Password, Dashlane, Keepass, RememBear. 57, 66, 201

PCFG Probablisitic Context-Free Grammar. Statistical grammar model. In password studies, PCFG algorithms can be adapted to measure the guessability of a given password and calculate a guess number.. 41, 67, 201

PD Persuasive Design. 61, 201

persona Fictional character that represents a market or user segment during a user-centered design process. 128, 201

PGS Password Guessing Service. Service that 'estimates plaintext passwords' guessability: how many guesses a particular password-cracking algorithm with particular training data would take to guess a password. https://pgs.ece.cmu.edu/. 41, 90, 201

PII personally identifiable information. 166, 201

PSM password strength meter. 64, 201

PWM password manager. 49, 50, 57, 61–64, 124–126, 133, 135, 136, 138, 201

REML Restricted maximum likelihood. 201

SeBIS Security Behavior Intentions Scale. 42, 128, 201

service provider Entity providing access to a resource through a specific service, e.g. the operator of a news website.. 4, 11, 43, 44, 50, 54, 60, 96, 201

SSO Single-Sign On. 43, 79, 95, 201

Unicode TODO. 201

USEC Usable Security and Privacy. 40, 41, 44, 150, 163, 201

UX user experience. 173, 201

W3C World Wide Web Consortium. 174, 201

WPA WiFi Protected Access. Protocol used in access control for wireless networks.. 9, 201

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] Mohammed A Fadhil Al-husainy and Raghda Ahmed Malih. 2015. Using Emoji Pictures To Strengthen the Immunity of Passwords Against Attackers. *European Scientific Journal* 11, 30 (2015), 153–165.

[10] Fatma Al Maqbali and Chris J Mitchell. 2016. Password Generators: Old Ideas and New. In *Proceedings of the Workshop on Information Security Theory and Practice (WISTP '16)*, Sara Foresti and Javier Lopez (Eds.). Springer International Publishing, Heraklion, Crete, Greece, 245–253. DOI:http://dx.doi.org/10.1007/978-3-319-45931-8_16

[11] 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

[12] 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

[13] 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

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

[15] 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

[16] 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.

[17] Elizabeth B.-N.Sanders. 2002. From User-centered to Participatory Design Approaches. In *Design and the Social Sciences. Making Connections* (1 ed.), Jorge Frascara (Ed.). Taylor & Francis, London, United Kingdom, Chapter 1, 1–8. DOI:http://dx.doi.org/10.1201/9780203301302.ch1

[18] 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

[19] 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

[20] 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

[21] 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

[22] 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

[23] 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

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

[25] 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

[26] 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

[27] 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

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

[29] 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

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

[31] 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

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

[33] 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, San Francisco, CA, USA, 538–552. DOI:http://dx.doi.org/10.1109/SP.2012.49

[34] 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

[35] 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

[36] 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

[37] 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

[38] 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

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

[40] 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

[41] 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/

[42] 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

[43] 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

[44] 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

[45] 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

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

[47] 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

[48] 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

[49] 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)*. Internet Society, San Diego, CA, USA, 1–16. DOI: http://dx.doi.org/10.14722/ndss.2014.23268

[50] 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

[51] 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

[52] 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

[53] 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

[54] 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

[55] 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

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

[57] 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

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

[59] 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

[60] 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

[61] 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

[62] 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

[63] 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

[64] 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

[65] 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

[66] 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

[67] 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

[68] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014a. The Tangled Web of Password Reuse. In *Proceedings of Network and Distributed System Security Symposium (NDSS 14)*. Internet Society, San Diego, CA, USA, 23–26. http://www.jbonneau.com/doc/DBCBW14-NDSS-tangled

[69] 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

[70] Artiom Dashinsky. 2015. Why you should (not) use Emoji in your passwords. (2015). https://medium.com/@hvost/why-you-should-not-use-emojis-in-your-passwords-b8db0607e169

[71] 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

[72] 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

[73] 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

[74] 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

[75] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. Touch me once and I know it's you! Implicit Authentication based on Touch Screen Patterns. 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

[76] 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

[77] 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

[78] Alexander De Luca, Katja Hertzschuch, and Heinrich Hussmann. 2010a. ColorPIN - Securing PIN Entry Through Indirect Input. 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

[79] 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

[80] 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

[81] 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

[82] 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

[83] 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

[84] 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.

[85] 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

[86] 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

[87] 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

[88] 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

[89] 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

[90] 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

[91] 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.

[92] 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

[93] 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

[94] 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

[95] 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

[96] 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.

[97] 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

[98] 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

[99] 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

[100] 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

[101] emogi Research. 2016. 2016 Emoji Report. (2016). http://cdn.emogi.com/docs/reports/2016

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

[103] 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

[104] 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

[105] 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

[106] 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

[107] Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. 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

[108] 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

[109] 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

[110] 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

[111] 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/

[112] 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

[113] 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

[114] 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

[115] Dinei Florêncio, Cormac Herley, and Baris Coskun. 2007. Do strong web passwords accomplish anything?. In *Proceedings of the USENIX Workshop on Hot Topics in Security (HotSec '07)*. USENIX Association, 10. http://portal.acm.org/citation.cfm?id=1361419.1361429

[116] 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.

[117] 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

[118] 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

[119] 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

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

[121] 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

[122] 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, 3759–3764. DOI:http://dx.doi.org/10.1145/1358628.1358926

[123] 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

[124] 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.

[125] 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

[126] 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

[127] 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/

[128] 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

[129] 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

[130] 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

[131] 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

[132] 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.

[133] 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

[134] 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

[135] 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

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

[137] 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

[138] 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

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

[140] 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

[141] 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

[142] 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

[143] 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

[144] 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.

[145] 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

[146] 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

[147] 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

[148] 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

[149] 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*. ACM, Rio de Janeiro, Brazil, 737–744. DOI:http://dx.doi.org/10.1145/2487788.2488034

[150] 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

[151] 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

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

[153] 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

[154] 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

[155] 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

[156] 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 *Proceedings of the Tenth Symposium On Usable Privacy and Security (SOUPS '14)*. USENIX Association, Menlo Park, CA, USA, 213–230. https://www.usenix.org/conference/soups2014/proceedings/presentation/harbach

[157] 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

[158] 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

[159] Eiji Hayashi, Rachna Dhamija, Nicolas Christin, and Adrian Perrig. 2008. Use Your Illusion: Secure Authentication Usable Anywhere. 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

[160] 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

[161] 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

[162] 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.

[163] 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

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

[165] 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

[166] 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

[167] 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.

[168] 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

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

[170] 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

[171] 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

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

[173] 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

[174] 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

[175] 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

[176] 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.

[177] 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

[178] 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

[179] 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.

[180] 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

[181] 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

[182] 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.

[183] 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

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

[185] 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.

[186] 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

[187] 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

[188] 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

[189] 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

[190] 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

[191] 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

[192] Warut Khern-am nuai, Weining Yang, and Ninghui Li. 2017a. Designing Better Password Strength Meters by Incorporating Contextual Information. *SSRN Electronic Journal* 2017, 05 (2017). DOI:http://dx.doi.org/10.2139/ssrn.2800499

[193] Warut Khern-am nuai, Weining Yang, and Ninghui Li. 2017b. 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

[194] 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

[195] 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

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

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

[198] 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

[199] 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: Measuring the Effect of Password-Composition Policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, Vancouver, BC, Canada, 2595–2604. DOI:http://dx.doi.org/10.1145/1978942.1979321

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

[201] 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

[202] 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

[203] 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

[204] 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.

[205] 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)*. Pittsburg, PA, USA, 67–78. DOI:http://dx.doi.org/10.1145/1143120.1143129

[206] 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

[207] 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

[208] 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

[209] 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

[210] 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

[211] 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

[212] 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.

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

[214] 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

[215] 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

[216] 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

[217] 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/

[218] 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

[219] 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

[220] 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

[221] 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

[222] 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

[223] 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

[224] 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

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

[226] 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

[227] 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.

[228] 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

[229] 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

[230] 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.

[231] Hannah Miller, Jacob Thebault-Spieker, Shuo Chang, Isaac Johnson, Loren Terveen, and Brent Hecht. 2015. "Blissfully happy" or "ready to fight": Varying Interpretations of Emoji. *GroupLens Research, University of Minnesota* (2015).

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

[233] 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

[234] 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

[235] 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

[236] 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

[237] 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

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

[239] 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

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

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

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

[243] 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

[244] Caroline Olsienkiewicz. 2016. *Verbesserung von verbalem Echtzeitfeedback bei der Passwortselektion*. Bachelor Thesis. Ludwig-Maximilians-Universität München.

[245] 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

[246] 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

[247] 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

[248] 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.

[249] 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

[250] 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

[251] 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

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

[253] 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.

[254] 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

[255] 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

[256] 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

[257] 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

[258] 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

[259] 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

[260] 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

[261] 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

[262] 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.

[263] 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

[264] 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

[265] 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

[266] 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

[267] 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

[268] 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

[269] 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

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

[271] 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

[272] 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/

[273] 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.

[274] 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

[275] 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

[276] 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

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

[278] 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

[279] Katharina Schwarz. 2016. *Partizipatives Design eines Registrierungsformulars mit nonverbalen persuasiven Elementen zur Passwortverbesserung*. Bachelor Thesis. Ludwig-Maximilians-Universität München.

[280] 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

[281] 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

[282] Tobias Seitz. 2017. Personalizing Password Policies and Strength Feedback. In *Proceedings of the Second International Workshop on Personalization in Persuasive Technology co-located with the 12th International Conference on Persuasive Technology*. CEUR, Amsterdam, The Netherlands, 64–69.

[283] Tobias Seitz, Manuel Hartmann, Jakob Pfab, and Samuel Souque. 2017a. 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, Denver, CO, USA, 2056–2063. DOI:http://dx.doi.org/10.1145/3027063.3053100

[284] Tobias Seitz and Heinrich Hussmann. 2017. PASDJO: Quantifying Password Strength Perceptions with an Online Game. In *Proceedings of the 29th Australian Conference on Computer-Human Interaction - OZCHI '17*. ACM Press, Brisbane, Australia, 117–125. DOI:http://dx.doi.org/10.1145/3152771.3152784

[285] Tobias Seitz, Florian Mathis, and Heinrich Hussmann. 2017b. The Bird is The Word: A Usability Evaluation of Emojis inside Text Passwords. In *Proceedings of the 29th Australian Conference on Computer-Human Interaction - OZCHI '17*. ACM Press, New York, New York, USA, 10–20. DOI:http://dx.doi.org/10.1145/3152771.3152773

[286] 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

[287] 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

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

[289] 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

[290] 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

[291] 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

[292] 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

[293] 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

[294] 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

[295] 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, Seoul, South Korea, 2903–2912. DOI:http://dx.doi.org/10.1145/2702123.2702586

[296] 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

[297] 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

[298] 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

[299] 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.

[300] 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

[301] Magdalena Siferlinger. 2017. *Unterstützung bei der strategischen Wiederverwendung von Passwörtern*. Bachelor Thesis. Ludwig-Maximilians-Universität München.

[302] 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

[303] 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

[304] 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

[305] 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

[306] 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

[307] 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

[308] 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

[309] 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

[310] 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

[311] 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

[312] 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.

[313] Elizabeth Stobert and Robert Biddle. 2015. Expert Password Management. In *Proceedings of Passwords 2015*. Springer International Publishing, Cambridge, UK, 3–20. DOI:http://dx.doi.org/10.1007/978-3-319-29938-9_1

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

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

[316] 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

[317] Anselm Strauss and Juliet M. Corbin. 1990. *Basics of qualitative research: grounded theory procedure and techniques*. Vol. 13. SAGE Publications. 3–21 pages.

[318] 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

[319] 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

[320] 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

[321] Caroline Taggart. 2015. *New Words for Old: Recycling Our Language for the Modern World*. Michael O'Mara Books. 192 pages. https://books.google.de/books?id=VPO4CgAAQBAJ

[322] 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

[323] 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

[324] 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

[325] 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

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

[327] 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

[328] 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

[329] 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

[330] 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

[331] Garreth W Tigwell and David R. Flatla. 2016. "Oh that' s what you meant!": Reducing Emoji Misunderstanding. In *Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct (MobileHCI '16)*. ACM, Copenhagen, Denmark, 859–866. DOI:http://dx.doi.org/2957265.2961844

[332] 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

[333] 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

[334] 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

[335] 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

[336] 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

[337] 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

[338] 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

[339] 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

[340] 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. https://www.usenix.org/system/files/login/issues/login

[341] 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.

[342] 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

[343] 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

[344] 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

[345] 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

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

[347] 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

[348] 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

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

[350] 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, Cape Town, South Africa, 460–467. DOI:http://dx.doi.org/10.1007/978-3-642-40477-1_28

[351] 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

[352] 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

[353] 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

[354] 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

[355] Ding Wang, Haibo Cheng, and Ping Wang. 2015. *Understanding Passwords of Chinese Users : Characteristics , Security and Implications*. Technical Report. 20 pages. https://www.researchgate.net/profile/Ding

[356] 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

[357] 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

[358] 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

[359] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. 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.

[360] 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

[361] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. 2010. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the 17th ACM conference on Computer and communications security - CCS '10*. ACM Press, Chicago, Illinois, USA, 162–175. DOI:http://dx.doi.org/10.1145/1866307.1866327

[362] 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

[363] 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

[364] 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

[365] 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

[366] 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

[367] 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

[368] 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

[369] 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

[370] Craig Wigginton, 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

[371] Sanjaya Wijeratne, Lakshika Balasuriya, Amit Sheth, and Derek Doran. 2010. EmojiNet : An Open Service and API for Emoji Sense Discovery. (2010).

[372] 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, San Diego, CA, USA, 1–12.

[373] 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

[374] 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

[375] 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

[376] 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

[377] 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, Vienna, Austria, 1216–1229. DOI:http://dx.doi.org/10.1145/2976749.2978346

[378] 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

[379] 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

[380] 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

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

[382] 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

[383] 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

[384] 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

[385] 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