



# Studying the Impact of Managers on Password Strength and Reuse

Authors: Sanam Ghorbani Lyastani\*, Michael Schilling†, Sascha Fahl‡, Sven Bugiel\*, Michael Backes\*  
CISPA, Saarland University, †Saarland University, ‡Leibniz University Hannover, §CISPA Helmholtz Center i.G.

Presented by: Nomaan Dossaji

# Passwords History

- Default authentication method
- Poor security... Why?
- Weak passwords
- Re-use passwords
- Solution -> Password managers
  - Less re-use since you do not have to remember the password
  - Generate strong passwords



# Most Common Passwords

1. 123456
2. Password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou



# Study Overview

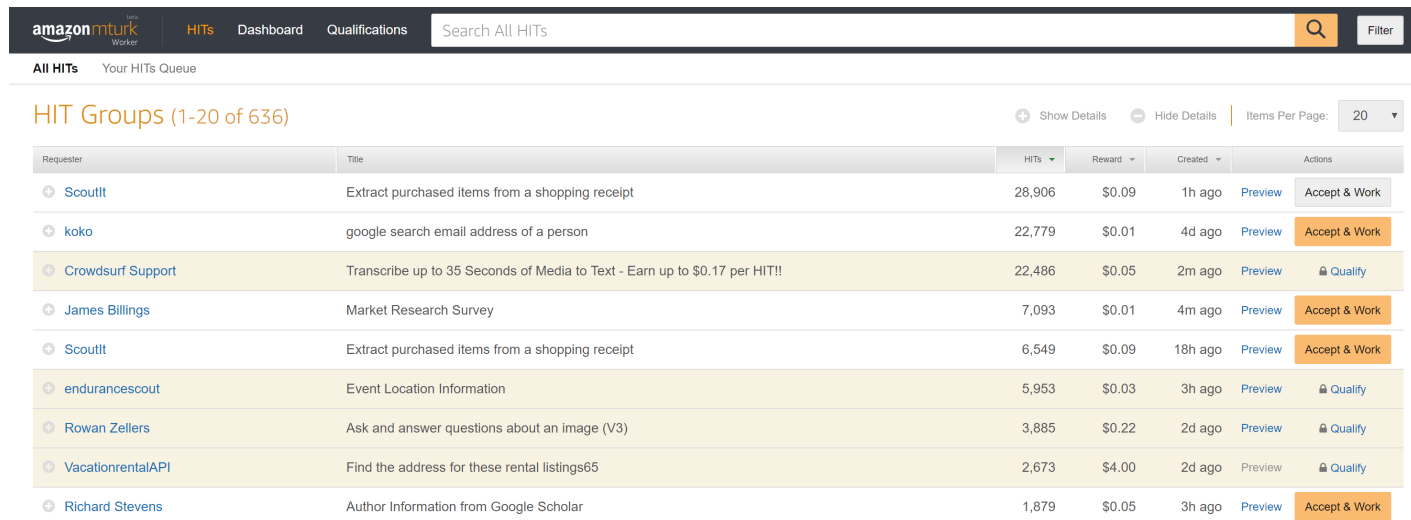
Using Amazon Mechanical Turk

1. Initial survey sampling
2. Collection of password metrics
3. Exit survey



# Amazon Mechanical Turk

- Web service enables companies to programmatically access this marketplace and a diverse, on-demand workforce



The screenshot shows the Amazon Mechanical Turk interface for viewing HITs. At the top, there's a navigation bar with 'amazonmturk Worker', 'HITS', 'Dashboard', and 'Qualifications'. A search bar labeled 'Search All HITs' is on the right. Below the navigation bar, there are tabs for 'All HITs' and 'Your HITs Queue'. The main content area is titled 'HIT Groups (1-20 of 636)'. It includes a table with columns for Requester, Title, HITs, Reward, Created, and Actions. The table lists 10 HIT groups with details like requester name, task title, number of HITs, reward, creation time, and action buttons (Preview, Accept & Work, Qualify).

Requester	Title	HITs	Reward	Created	Actions
ScoutIt	Extract purchased items from a shopping receipt	28,906	\$0.09	1h ago	<a href="#">Preview</a> <a href="#">Accept &amp; Work</a>
koko	google search email address of a person	22,779	\$0.01	4d ago	<a href="#">Preview</a> <a href="#">Accept &amp; Work</a>
Crowdsurf Support	Transcribe up to 35 Seconds of Media to Text - Earn up to \$0.17 per HIT!!	22,486	\$0.05	2m ago	<a href="#">Preview</a> <a href="#">Qualify</a>
James Billings	Market Research Survey	7,093	\$0.01	4m ago	<a href="#">Preview</a> <a href="#">Accept &amp; Work</a>
ScoutIt	Extract purchased items from a shopping receipt	6,549	\$0.09	18h ago	<a href="#">Preview</a> <a href="#">Accept &amp; Work</a>
endurancescout	Event Location Information	5,953	\$0.03	3h ago	<a href="#">Preview</a> <a href="#">Qualify</a>
Rowan Zellers	Ask and answer questions about an image (V3)	3,885	\$0.22	2d ago	<a href="#">Preview</a> <a href="#">Qualify</a>
VacationrentalAPI	Find the address for these rental listings65	2,673	\$4.00	2d ago	<a href="#">Preview</a> <a href="#">Qualify</a>
Richard Stevens	Author Information from Google Scholar	1,879	\$0.05	3h ago	<a href="#">Preview</a> <a href="#">Accept &amp; Work</a>



# Initial Survey

- 31-34 questions on password behavior
  - How does the participant create and manage their passwords
  - Demographic questions
- Obtain general idea of common password creation and storage in the public
- Reduce bias using these questions
- Participant Criteria
  - Located in US, 100+ previously approved tasks/70% all of tasks, 18+ years old
- Participants received \$4
- 505 participants, reliable data = 476



# Study Statistics

- 476 participants for a survey
- Determine strategies for:
  - Creating a password
  - Storing a password
  - Attitudes toward passwords
  - Past experience with password leaks and password managers
- Classify 2 groups: password manager users and users that don't have help for password creation



# Study Follow-up

- Invited 364, 174 started, and 170 finished
- 170 participants recruited -> 49 use password managers
- Chrome browser plugin for password manager users to collect password metrics and questionnaire on passwords
- Participants paid \$20 when finished
- Ask participants to re login to websites that stay logged into





# Chrome Plug-In

- Monitors input to password fields and sends metrics back to server
- Metrics:
  - Length of password and frequency of each character
  - Password strength (Shannon, NIST entropy and zxcvbn score)
  - Website category
  - Entry method (human, Chrome password manager, copy&paste, 3<sup>rd</sup> party password manager plug-in, external password manager program)
  - Questionnaire (website's value for privacy)
  - Hashes (password and 4 character substring)



# zxcvbn

- More reliable than Shannon or NIST
- Uses pattern matching, password dictionaries, and mangling rules to determine crackability of passwords
- Scales password strength from 0 (weakest) to 4 (strongest)
- Ex) !@#\$%^&\*() score 1 since straight row of keys
- Ex) AiWuutaiveep9 score 4 and randomly generated



# Password Entry Method

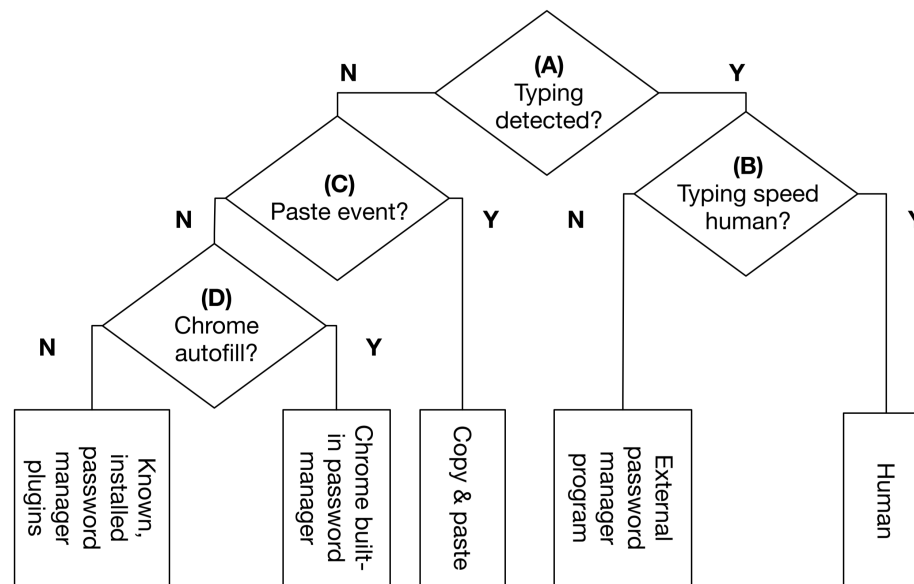


Figure 2. Decision tree of our plugin to detect password entry methods

# Plug-In Questionnaire

**Question 1:** Did you successfully login to twitter.com?

Yes      No  
☐      ☐

**Question 2:** How stronge/secure do you think the password is that you just have entered on this website?

       
☆☆☆☆☆   ☆☆☆☆☆   ☆☆☆☆☆   ☆☆☆☆☆   ☆☆☆☆☆   N/A  
☐      ☐      ☐      ☐      ☐      ☐

**Question 3:** Do you agree with these statements?

Strongly  
Disagree   Disagree   Neutral   Agree   Strongly  
Agree   N/A

The current website handles privacy sensitive information.

☐

☐

☐

☐

☐

☐

If someone steals your password for this website, they can harm you (e.g., financially, social reputation, use services, etc).

☐

☐

☐

☐

☐

☐

# Privacy Concerns

- Show source code to users with IT background
- Explain purpose of study with high transparency
- Only take website category
- Only send information if user fills out questionnaire
- Show user what information is being sent
- Only collect successful login, no website browsing
- Only take the hashes of passwords



# Privacy Concerns Cont.

**Note:** You will see this pop-up for this URL (twitter.com) only once. Please answer all questions properly.

**Privacy Protection Note:** We never store your password anywhere! If you are interested in which data we collect, we explain it [here](#) in detail.

Privacy Protection Note

To protect your data, we **never** store or send your plain passwords. This is what we collect for the current website twitter.com. For more details you can check our website [here](#).

Password Length	10	Password Manager	No Password Manager
Upper Case Letters	1	NIST Entropy	24
Lower Case Letters	7	zxcvbn Score	3
Special Chars	0	Shannon Entropy	32
Numbers	2	Website category	2995
Hash (PBKDF2) e92e9046d088f128b71b2363dd69aa424e574f7c8318089a1c0fe8d5e173aa49			

The current website handles privacy sensitive information.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If someone steals your password for this website, they can harm you (e.g., financially, social reputation, use services, etc).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 4. Notice by our plugin about the collected data for the current website.

I

# Exit Survey

- 113 workers invited and 109 workers accepted
- \$1.50 compensation for completing survey
- Invite workers from Chrome plug-in that do not use extra password manager software
- Have they used external password manager software, if so why don't they still use it?



# Basic Statistics

- Significant correlation between password strength and reuse

Table VI

SUMMARY STATISTICS FOR ALL 170 PARTICIPANTS IN OUR PLUGIN-BASED DATA COLLECTION. LIKE [50], WE FIRST COMPUTED MEANS FOR EACH PARTICIPANT AND THEN COMPUTED THE MEAN, MEDIAN, STANDARD DEVIATION, AND MIN/MAX VALUES OF THOSE MEANS.

Statistic	Mean	Median	SD	Min	Max
Number of passwords	10.39	9.00	5.52	1.00	27.00
Entry methods	2.24	2.00	0.75	1.00	4.00
Percentage reused passwords					
Non-reused	29.44%	21.58%	28.25%	0.00%	100.00%
Only-exact-reused	15.72%	0.00%	24.43%	0.00%	100.00%
Only-partially-reused	18.38%	11.11%	19.88%	0.00%	100.00%
Exact-and-partial reused	36.46%	38.75%	30.88%	0.00%	100.00%
Password composition					
Length	9.61	9.29	1.72	6.33	16.86
Character classes	2.52	2.50	0.58	1.00	3.94
Digits	2.54	2.38	1.24	0.25	6.73
Uppercase letters	0.85	0.67	0.81	0.00	4.62
Lowercase letters	5.92	5.72	1.96	1.67	15.50
Special characters	0.30	0.10	0.54	0.00	5.19
Password strength					
Zxcvbn score	2.20	2.14	0.75	0.67	4.00
Shannon entropy	29.31	28.37	7.93	16.00	68.00
NIST entropy	23.50	23.00	2.98	17.17	35.69





# Plug-In Metrics

Table VII  
NUMBER OF DISTINCT PASSWORD ENTRIES WITH EACH ENTRY METHOD.

Entry method	All passwords	Unique passwords
Chrome auto-fill	949 (53.71%)	540 (51.67%)
Human	590 (33.39%)	331 (31.67%)
LastPass plugin	128 (7.24%)	100 (9.57%)
Copy&paste	55 (3.11%)	51 (4.88%)
Unknown plugin	41 (2.32%)	23 (2.20%)
External manager	4 (0.23%)	0 (0.00%)
$\Sigma$	1,767	1,045

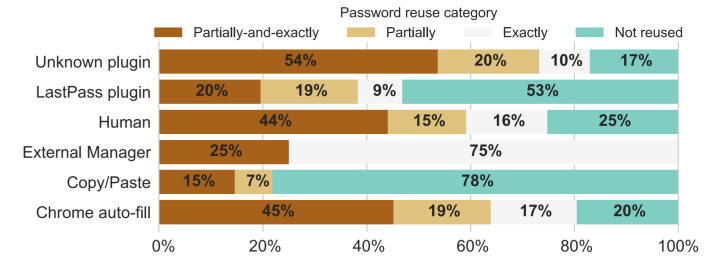


Figure 5. Breakdown of password reuse by entry method for all passwords.

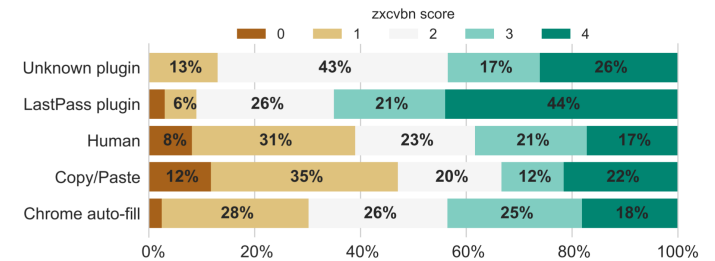


Figure 6. Breakdown of zxcvbn scores per entry method for unique passwords.

# Grouping of Participants

- Split the participants into 2 groups
- Password Managers/Generators (PWM): Those who reported using an external password manager or a password generator in initial survey
- Human-Generated (Human): Those who generate their passwords using a strategy that does not involve technical means

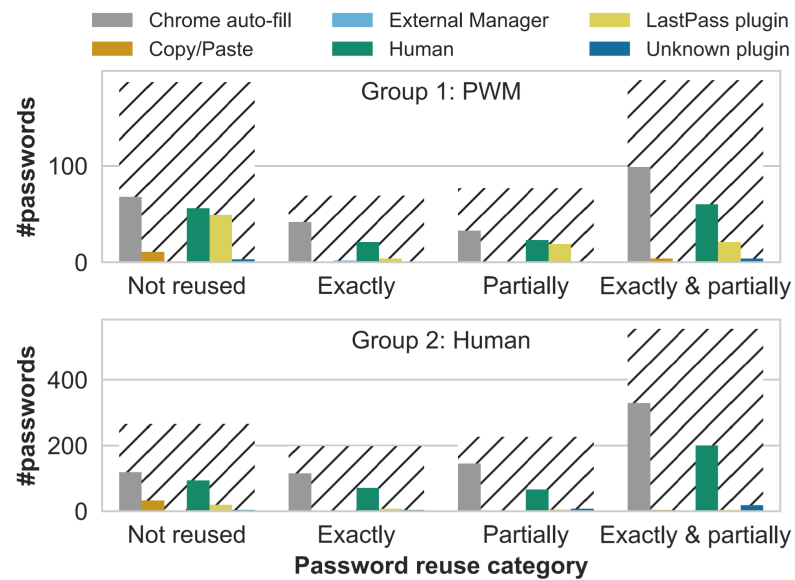


Figure 8. Distribution of password reuse categories by participant group and broken down by detected entry method. Hatched bars show total number of passwords per category. (Note the different y-axis limits)

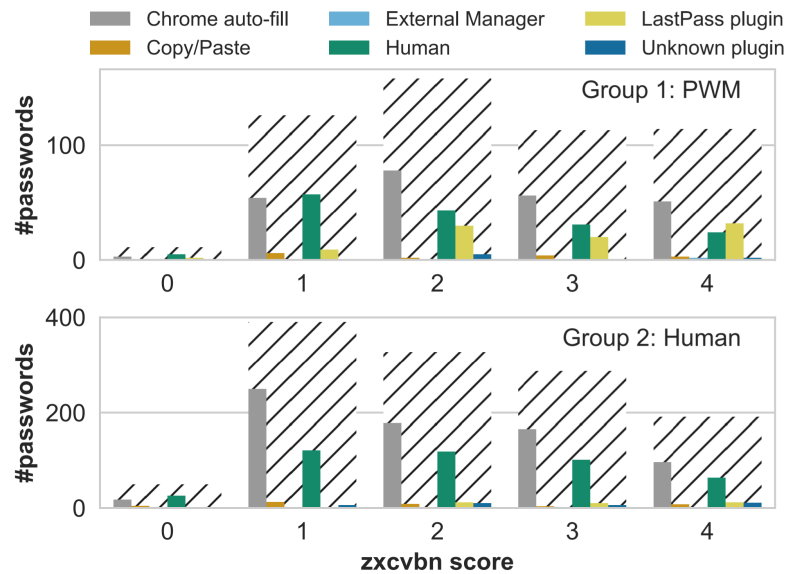


Figure 7. Password strength distribution by participant group and broken down by detected entry method. Hatched bars show total number of passwords per score. (Note the different y-axis limits)

# Regression Model

- First test basic multi-level models for password reuse and strength without any explanatory variables
  - Extend models by adding sets of predictors
1. Login Level:
    - a) Entry method
    - b) Website value to participant
    - c) Self-reported password strength
  2. User Level:
    - a) Number of submitted passwords per user
    - b) Password creation strategy
    - c) Password management strategy
  3. Cross Level interactions between user's password creation strategy and entry method



# Method to Pick Model

- AIC - Akaike Information Criterion
  - Estimates quality of model to data
  - Lower the better

Table XII

GOODNESS OF FIT FOR THE MODELS PREDICTING ZCVBN SCORES

	AIC	logLik	df	Pr(>Chisq)
simple regression	5080.6	-2536.3		
multi-level base	4536.7	-2263.4	1	<0.001
+ login level	4316.3	-2147.1	6	<0.001
+ user level	4320.4	-2143.2	6	0.2494034
+ interactions	4309.5	-2133.7	4	<0.001

Table XIII

GOODNESS OF FIT FOR THE MODELS PREDICTING PASSWORD REUSE

	AIC	logLik	Df	Pr(>Chisq)
simple regression	1959.7	-978.84		
multi-level base	1794.6	-895.28	1	< 0.001
+ login level	1694.9	-839.46	6	< 0.001
+ user level	1684.7	-828.37	6	<0.01
+ interactions	1687.6	-825.80	4	0.27351

# Zxcvbn Model

- Self-reported password strength is a significant predictor of actual password strength
- Password entry method alone was not a significant predictor
- Password entry method AND creation strategy was, however, are significant predictors



# Password Reuse Model

- Significantly influenced by entry method
  - Compared to human entry odds:
    - 2.85x lower when using LastPass plug-in
    - 14.29x lower with copy&paste
- Passwords from those who use password generators are 3.7x more likely to not be reused
- Passwords less likely to be reused:
  - Passwords entered into a website with higher value
  - Passwords that users considered strong
  - People who used analog password storage



# Password Reuse Model Cont.

- Compared to human entry odds, 1.65x more likely to reuse with Chrome autofill
- With more passwords, it is more likely to reuse passwords





# Participants Background

Table IX  
DEMOGRAPHICS OF OUR TWO PARTICIPANT CATEGORIES.

	Human	PWM
Number of participants	121	49
Gender		
Female	59 (48.76%)	14 (28.57%)
Male	62 (51.24%)	35 (71.43%)
Age group		
18–30	48 (39.67%)	16 (32.65%)
31–40	39 (32.23%)	24 (48.98%)
41–50	27 (22.31%)	5 (10.20%)
51–60	5 (4.13%)	5 (6.12%)
61–70	2 (1.65%)	0
≥71	0	1 (2.04%)
Computer science background		
Yes	10 (8.26%)	17 (34.69%)
No	111 (91.74%)	32 (65.13%)
Education level		
Less than high school	0	1 (2.04%)
High school graduate	22 (18.18%)	4 (8.16%)
Some college, no degree	28 (23.14%)	6 (12.24%)
Associate's degree	27 (22.31%)	7 (14.29%)
Bachelor degree	35 (28.93%)	27 (55.10%)
Ph.D.	0	1 (2.04%)
Graduate/prof. degree	9 (7.44%)	3 (6.12%)
Ethnicity		
White/Caucasian	91 (75.21%)	32 (65.31%)
Black/African American	15 (12.40%)	10 (20.41%)
Asian	5 (4.13%)	4 (8.16%)
Hispanic/Latino	10 (8.26%)	2 (4.08%)
Multiracial	0	1 (2.04%)
Privacy concern (Westin index)		
Privacy fanatic	45 (37.19%)	21 (42.86%)
Privacy unconcerned	15 (12.40%)	16 (32.65%)
Privacy pragmatist	61 (50.41%)	12 (24.49%)
Attitude about passwords		
Pessimist	1 (0.83%)	2 (4.08%)
Optimist	88 (72.73%)	44 (89.80%)
Conflicted	32 (26.45%)	3 (6.12%)
Prior password leaked experienced		
No	53 (43.80%)	19 (38.78%)
Yes	44 (36.36%)	14 (28.57%)
Not aware of	24 (19.83%)	16 (32.65%)

Table X  
DISTRIBUTION OF ENTRY METHODS PER PARTICIPANT GROUP.

Entry method	Group 1 (PWM)	Group 2 (Human)
All passwords		
Chrome auto-fill	242 (46.36%)	707 (56.79%)
Human	160 (30.65%)	430 (34.54%)
LastPass plugin	93 (17.82%)	35 (2.81%)
Copy&paste	16 (3.07%)	39 (3.13%)
Unknown plugin	8 (1.53%)	33 (2.65%)
External manager	3 (0.57%)	1 (0.08%)
Σ	522	1245
Unique passwords		
Chrome auto-fill	144 (42.99%)	396 (55.77%)
Human	101 (30.15%)	230 (32.39%)
LastPass plugin	72 (21.49%)	28 (3.94%)
Copy&paste	14 (4.18%)	37 (5.21%)
Unknown plugin	4 (1.19%)	19 (2.68%)
Σ	335	710



# Analysis

- External password managers or copy&paste passwords lead to less password reuse
- Chrome autofill has more password reuse
- Password strength and reuse has a strong correlation
- Password reuse is common except for LastPass plug-in and copy&paste
- 80% Chrome autofill passwords reused
- 47% LastPass plug-in passwords reused
- LastPass had strongest average strength of passwords (2.80 mean)



# Exit Survey Result

Table XVI  
EXIT SURVEY'S RESULT

Users do not use any kind of 3rd party password managers because...	
the participants do not trust vendor/software	37.61%
they cost lots of money	20.18%
they are not really easy to set up/ easy to use	11.93%
of lack of synchronization between users' different device	7.34%
of lack of support for the user device	2.75%
Other Reasons	
Chrome's password saving feature suffices for the users	59.63%
can handle managing the password w/o manager	37.61%
did not think about it before	29.36%
not sure which one is better	24.77%

# Why Participants do not use PWM

- Single point of failure
- "I think that it saves time but also generates a way for hackers to steal the information for themselves."



# Limitations

- Not much discussion among password strength/reuse and website category
- Final survey assumes knowledge of 3<sup>rd</sup> party password managers



# Discussion

- What did you think about the survey?
- Stronger passwords are correlated with people with CS backgrounds... Is there a bias that CS backgrounds are more familiar with the risks of weak passwords?
- What could they have done better?
- What would be some good follow-up studies?



# Sources

- Lyastani, Sanam Ghorbani, Michael Schilling, Sascha Fahl, Sven Bugiel, and Michael Backes. "Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse." In 27th {USENIX} Security Symposium ({USENIX} Security 18). USENIX} Association}.
- Lyastani, Sanam Ghorbani, Michael Schilling, Sascha Fahl, Sven Bugiel, and Michael Backes. "Studying the Impact of Managers on Password Strength and Reuse." arXiv preprint arXiv:1712.08940 (2017).
- <http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/>