Table 2:
OLS regression of the complexity of the password (random password entropy, measured in bits) for a website based on how often that password is entered into the website or how often that website is visited

	Estimate	95% CI	
(Intercept)	52.09***	51.37	52.83
Password entries per day	0.24	−0.30	0.80
Webpage visits per day	−0.08*	−0.14	−0.01
Webpage visits per password entry	0.003*	0.000	0.005
R^2	0.00		

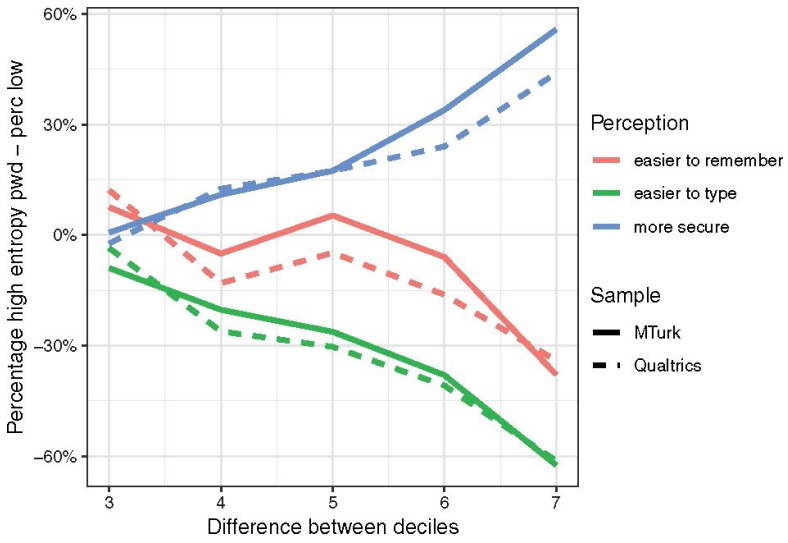
Significance codes: 0 “***” 0.001 “**” 0.01 “*” 0.05 “.” 0.1 “” 1.

Table 5:
Relationships between password complexity and importance, grouped by different categories of importance

Category	Correlation	95% CI	
Website overall	0.11***	0.06	0.16
Content on the website	0.09***	0.04	0.14
Whether you visit the website	0.06*	0.01	0.11
Personal information entered into website	0.02	−0.03	0.07

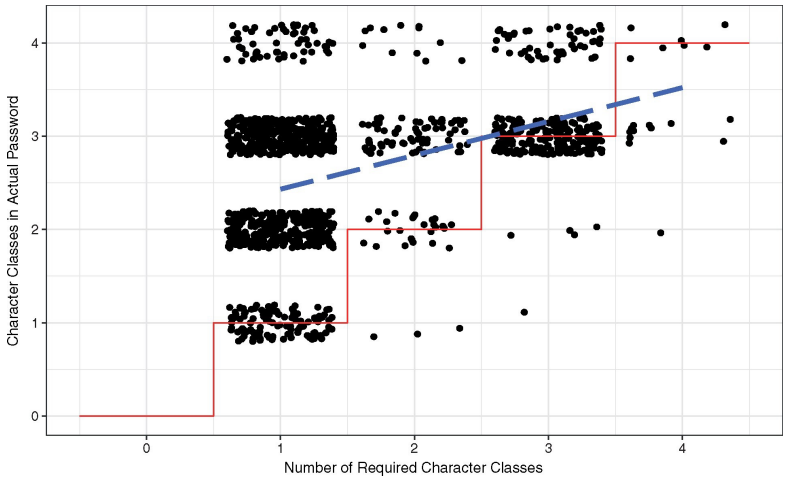
Significance codes: 0 “***” 0.001 “**” 0.01 “*” 0.05 “.” 0.1 “” 1.

Figure 1: Difference in password entropy (x-axis) by user interpretation of that difference (y-axis). The solid line is ...



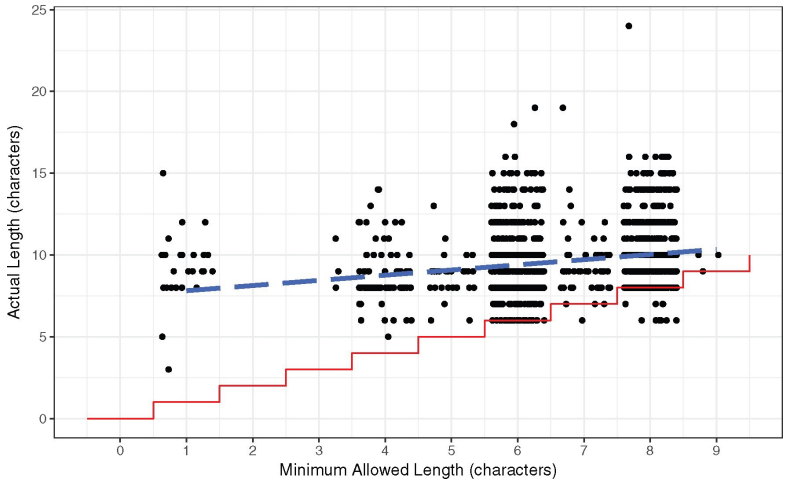
J Cyber Secur, Volume 7, Issue 1, 2021, tyab012, https://doi.org/10.1093/cybsec/tyab012
The content of this slide may be subject to copyright: please see the slide notes for details.

Figure 5: Required number of character classes in a password versus actual password character classes. The solid red ...



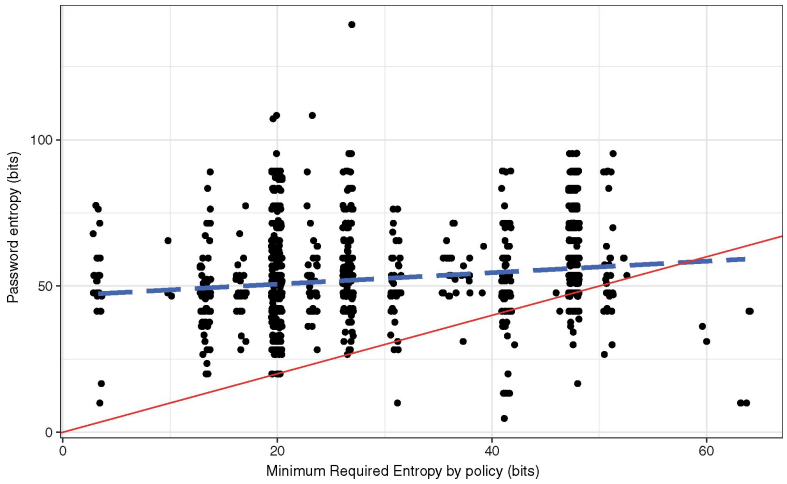
J Cyber Secur, Volume 7, Issue 1, 2021, tyab012, https://doi.org/10.1093/cybsec/tyab012
The content of this slide may be subject to copyright: please see the slide notes for details.

Figure 4: Required password length versus actual password length. The solid red line is the policy minimum and the ...



J Cyber Secur, Volume 7, Issue 1, 2021, tyab012, https://doi.org/10.1093/cybsec/tyab012
The content of this slide may be subject to copyright: please see the slide notes for details.

Figure 3: The relationship between password complexity (y-axis) and the minimum complexity required by the website's ...



J Cyber Secur, Volume 7, Issue 1, 2021, tyab012, https://doi.org/10.1093/cybsec/tyab012
The content of this slide may be subject to copyright: please see the slide notes for details.

Table 4:
Password complexity grouped by the quintile of importance, with larger numbers indicating higher importance

Quintile	Complexity	Importance
Low	51.0	2.65
	51.6	2.99
Medium	52.2	3.29
	54.2	3.48
High	54.6	3.65

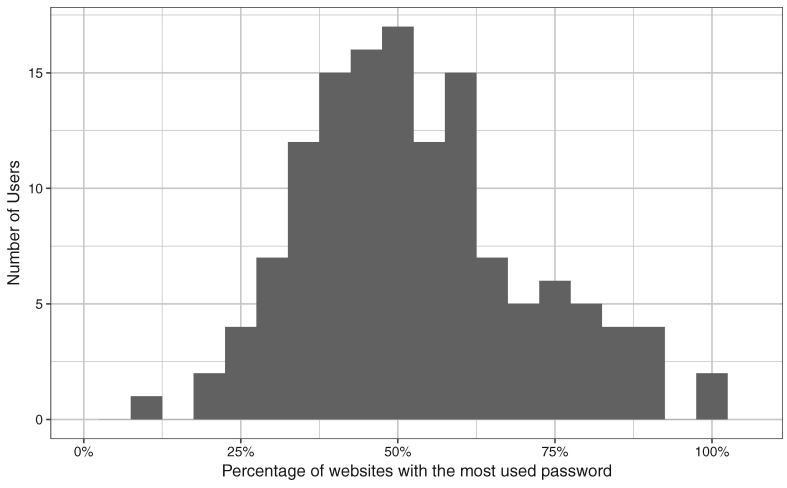
The importance numbers are the average importance for that quintile on a 5-point Likert scale, averaged across all 19 importance questions.

Table 3:
Average complexity (in bits) of passwords used on websites, by logical category of the website

Category	Complexity	Number of users
University	57.2	134
Economy and finance	55.1	56
Chat and messaging	55.1	18
News and media	54.3	11
Information tech	54.2	110
Media sharing	52.2	37
Education	51.7	123
Business	51.7	134
Streaming media	50.3	44
Shopping	50.0	112
Social networking	50.0	100
Entertainment	49.6	69
Uncategorized	48.2	105
Games	46.9	22
Sports	45.8	19
Travel	43.9	17

Only showing the 16 categories that at least 10 users visited; analyses were conducted with all 23 categories. Across all passwords, the average complexity was 49.5 bits. Each user may visit multiple websites in each category.

Figure 2: Histogram of often the most-common password is re-used.



The content of this slide may be subject to copyright: please see the slide notes for details.

OXFORD UNIVERSITY PRESS

Evidence about Password Use

A. “Out of the 134 users in this study, only 2 have exactly 1 password that they reuse everywhere (1.5% of users). These two users reused their single password on 10 and 18 different websites during the 6 weeks of the study.”

B. “The remaining 132 users all had more than one password that they had used, with different websites having different passwords. Most users had four to eight passwords”

C. “approximately half of our users (40%, 54 out of 134) using their most dominant password on fewer than 50% of the websites they have passwords on, and only 19 users (14%) using their most dominant password on 75% or more of websites.”

D. “On average, the passwords entered into websites have 21bits of complexity more than the password composition policy requires. This is a substantial difference; it roughly corresponds to the difference between a 7 character password (36bits of complexity) and an 11 character password (57bits of complexity), where the passwords are composed of lowercase letters and numbers.”

E. “Only 16.2% of passwords are at or below the minimum requirements for the website they are used in. A total of 42% of users (56 out of 134) don’t have a single password that is. at or below the minimum required complexity; all of their passwords are more complex than the website where they were used requires them to be.”

F. “For each participant, we calculated the combined complexity requirements of all of the websites where they used each of their passwords, and compared that to the complexity of the password that was chosen. Only 30% of reused passwords are at or below this combined minimum. This means that about 70% of passwords are more complex than required on all of the websites that they are used on.”

G. “Entering passwords can be a very time-consuming task; recent estimates suggest that it takes 10–14seconds to enter a password every time it is needed [27], and users enter a password approximately 3.2 times per day [2], which, when combined, suggest that users are spending over 3hours per year just entering passwords”

Evidence about Password Use

H. “We calculated the number of times a password was entered into each website and divided it by the number of days between the first and last uses of the website by that user. This gives us an estimate for how often a password needs to be entered —the number of password entries per day. This has very little correlation with the complexity of the password used ($r=0.00$, $P=0.72$, 95% CI: [-0.04, 0.03]).”

I. “Looking at how many webpages on the site the user is able to view before being asked to log in again. If, like one of our participants, you are able to view 10,000 different pages on reddit in 6weeks but are only asked to log in once, that may seem like a very efficient use of your time entering your password. We calculated the number of visits per password entry, but also found very little correlation with the complexity of the password used ($r(2531)=0.03$, $P=0.15$, 95% CI: [-0.01, 0.06]).”

J. “We also find a very small correlation here ($r(2531)=-0.03$, $P=0.16$, 95% CI: [-0.06, 0.01]) between the number of webpage visits per day on a website and the complexity of the password used on that website.”

K. “We found a positive correlation between these importance ratings and the complexity of passwords used on that website ($r(1517)=0.09$, $P<0.001$, 95% CI: [0.04, 0.14]).”