Understanding Password Re-Use

Rick Wash[a], Emilee Rader[a], Ruthie Berman[b], and Zac Wellmer[a]

[a]Michigan State University
[b]Macalester College

myspace

WHAT HAPPENED?

Shortly before the Memorial Day weekend (late May 2016), we became aware that stolen Myspace user login data was being made available in an online hacker forum.

Importantly, if you use passwords that are the same or similar to your Myspace password on other online services, we recommend you set new passwords on those accounts immediately.

myspace

LinkedIn

myspace

LinkedIn

tumblr.

PANDORA®

Dear Pandora listener:

You may have seen recent press articles indicating that LinkedIn was the victim of a data breach in 2012 in which over 100 million usernames and passwords were accessed and released onto the Internet last month.

Our security teams have analyzed the LinkedIn credential data and our analysis indicates that **your username was among those leaked onto the Internet.** This username is the same on LinkedIn and Pandora. While you have probably already changed your password on the LinkedIn website you should also change your password on any other website where you used the same password, including Pandora. Password reuse, using the same password across websites, is one way that malicious entities attempt to gain unauthorized access to services, which is why it's important to use different passwords with different accounts.

While there is no evidence that your account has been tampered with in any way, it is a best security practice to do a password reset in these situations. **Below is a link with which you can request a password reset on Pandora.**

PANDORA®

Dear Pandora listener:

"Our security teams have analyzed the LinkedIn credential data and our analysis indicates that your username was among those leaked onto the Internet."

While there is no evidence that your account has been tampered with in any way, it is a best security practice to do a password reset in these situations. **Below is a link with which you can request a password reset on Pandora.**

Don't use your MSU NetID and password for non-MSU accounts.

Passwords

Protect your NetID and password combination. Don't use your MSU NetID and password for social media sites, retail sites, or any non-MSU sites.

Reputable organizations will **NEVER** ask for your account and password combination in an email message.

Passphrase example

Even if your system does not support the length of a passphrase, a sentence can be the basis of a strong password.

How do people make choices about password re-use?

Study details

Browser Plugin

Observe ALL websites visited

Collect Password use:
Measure, hash password

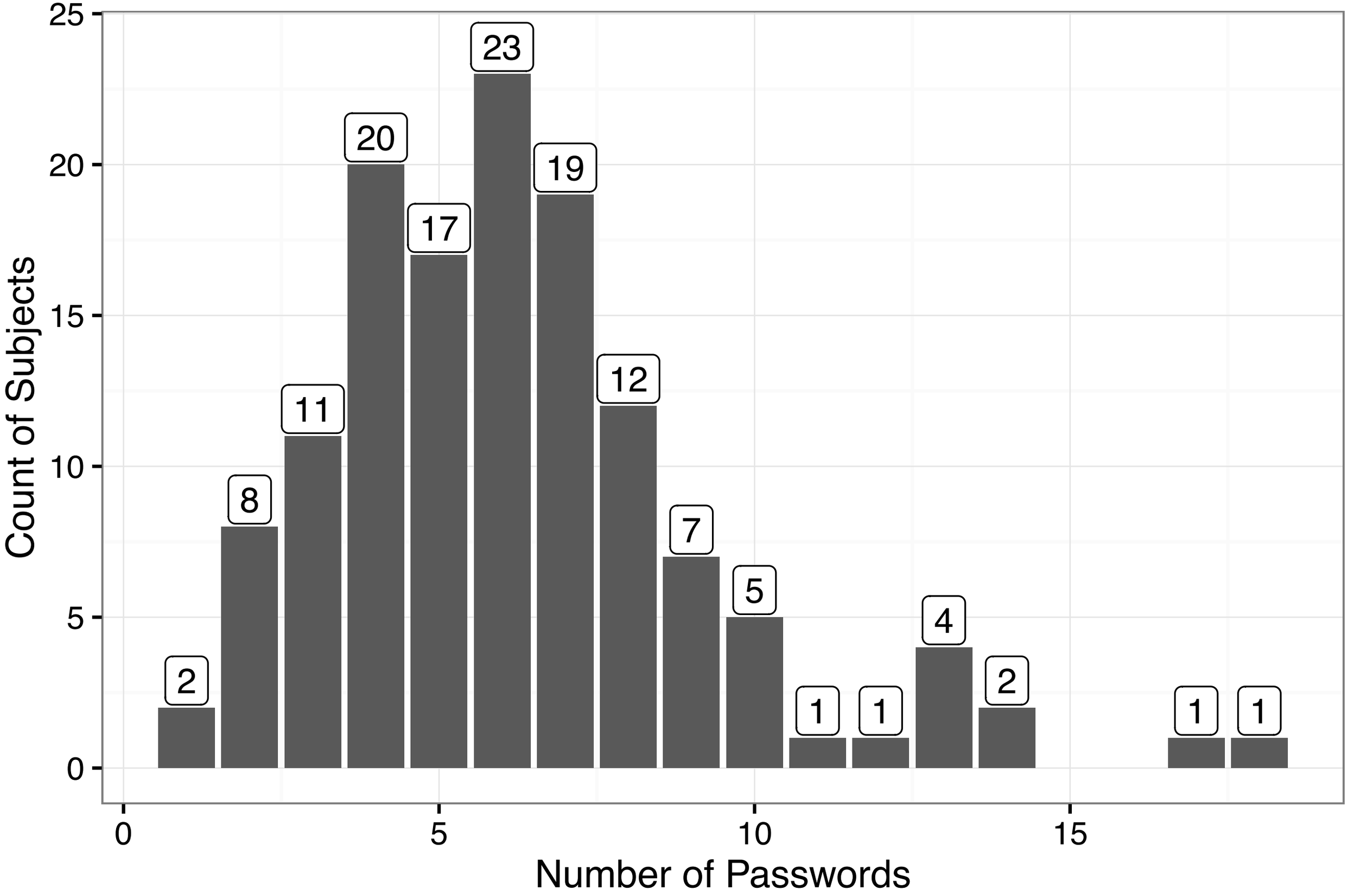
Study details

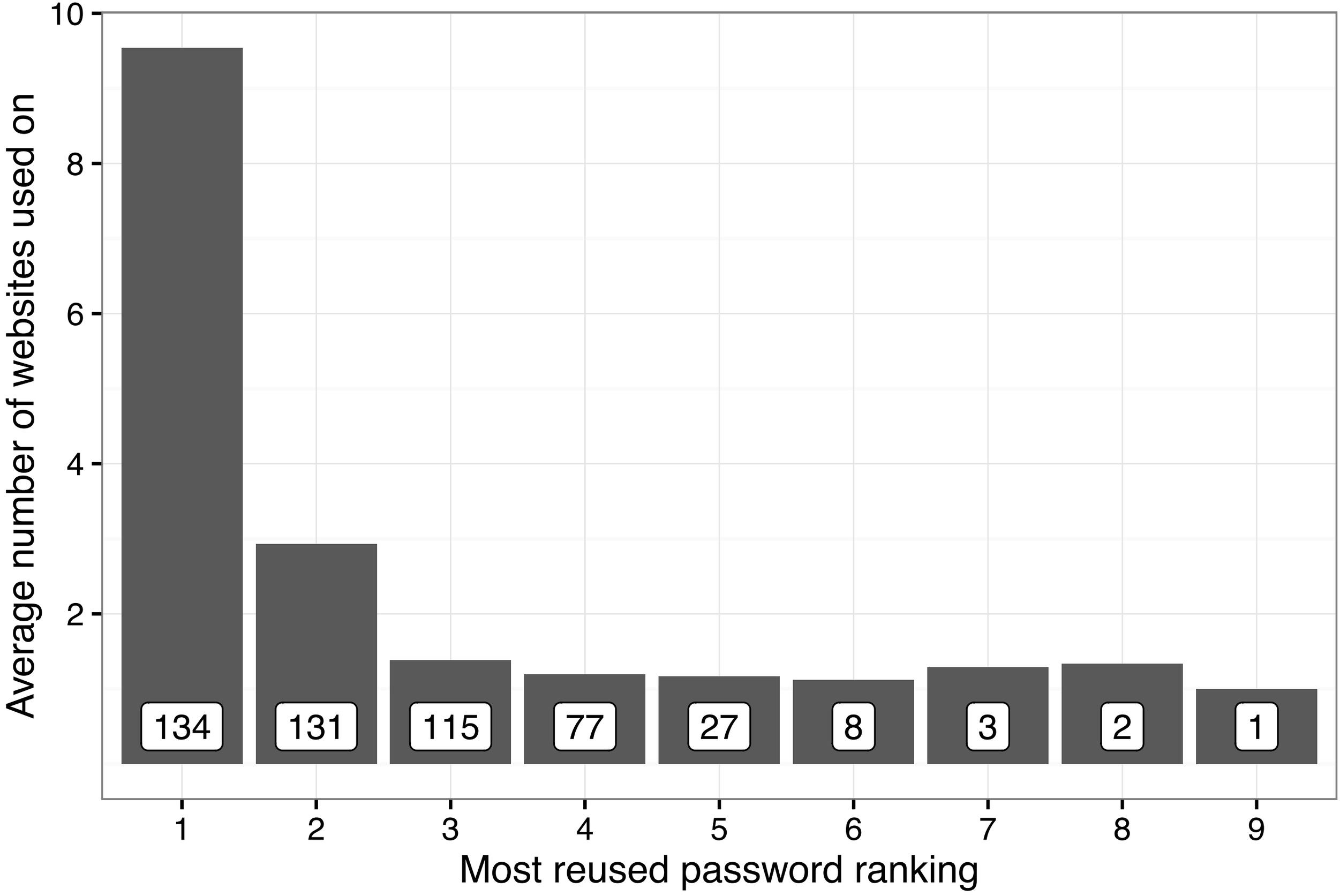
134 University Students
(Excluding Comp Sci)

Collected data for 6 weeks

53% Women
46% Men

$70 compensation

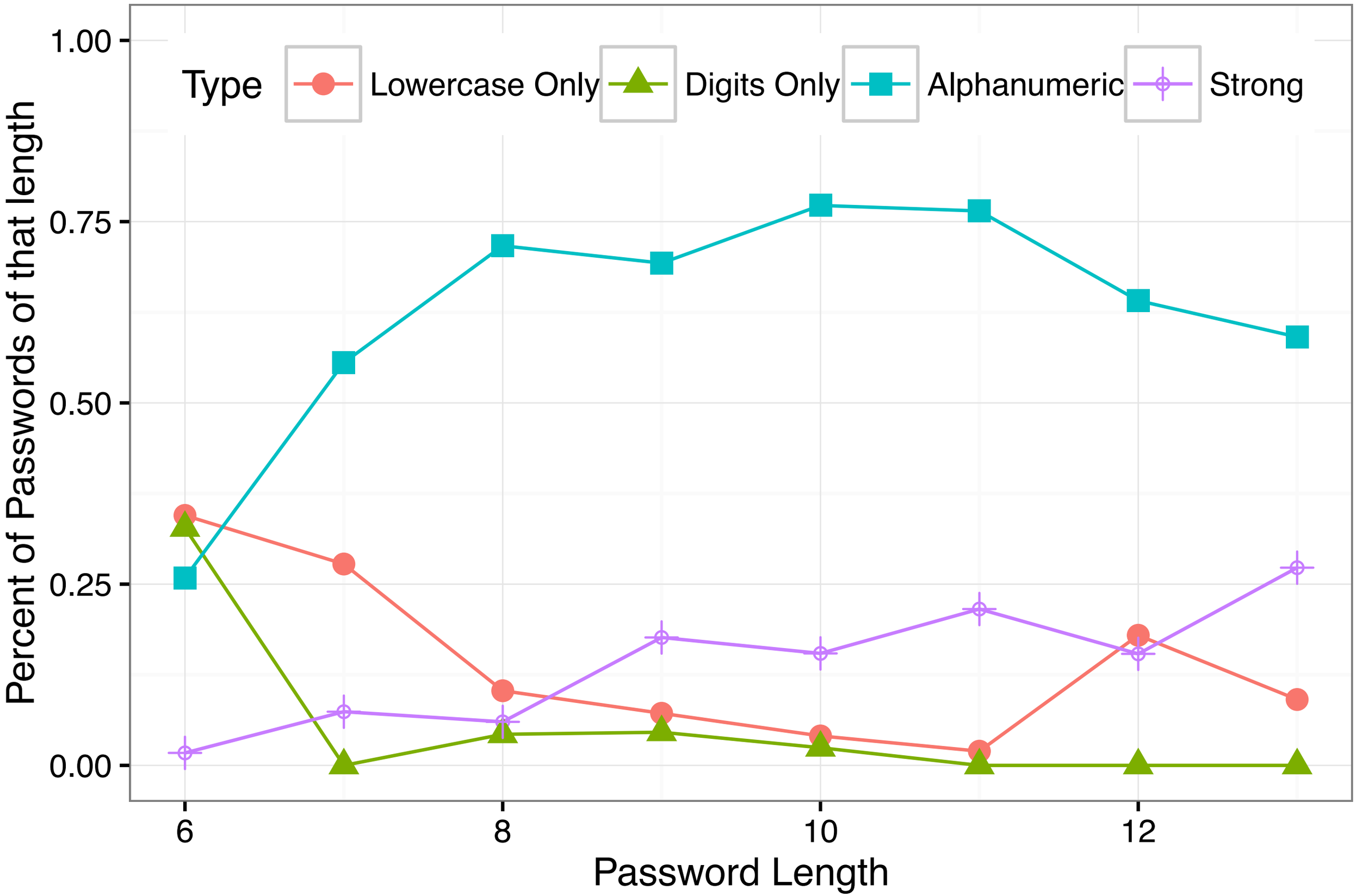

Count of Subjects
25
20
15
10
5
0
2
8
11
20
17
23
19
12
7
5
1
1
4
2
1
1
0
5
10
15
Number of Passwords


Average number of websites used on
10
8
6
4
2
134
131
115
77
27
8
3
2
1
1
2
3
4
5
6
7
8
9
Most reused password ranking

What passwords get re-used?

Throw-away Password?

Best password?


Type
Lowercase Only
Digits Only
Alphanumeric
Strong
1.00
0.75
0.50
0.25
0.00
Percent of Passwords of that length
6
8
10
12
Password Length

	Password Re-used?
(Intercept)	-1.07 ***
Complexity Ranking	-0.04 **
Times entered into each website	0.18 ***
Uses a Password Manager	0.00
$R^2_{GLMM_C}$	0.32

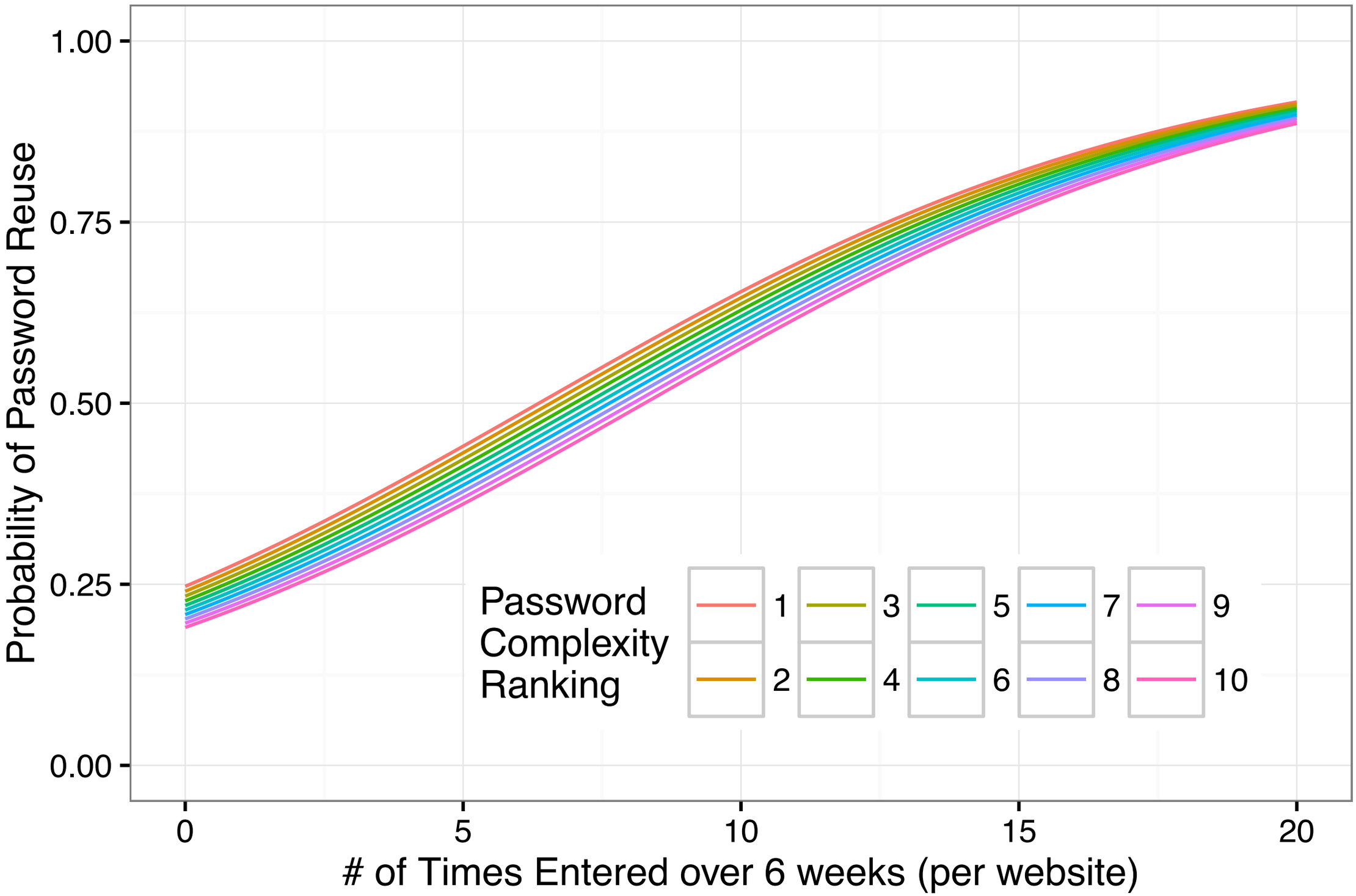
People re-use complex passwords

	Password Re-used?
(Intercept)	-1.07 ***
Complexity Ranking	-0.04 **
Times entered into each website	0.18 ***
Uses a Password Manager	0.00
$R^2_{GLMM_C}$	0.32

People re-use frequently entered passwords

	Password Re-used?
(Intercept)	-1.07 ***
Complexity Ranking	-0.04 **
Times entered into each website	0.18 ***
Uses a Password Manager	0.00
$R^2_{GLMM_C}$	0.32

People re-use frequently entered passwords



Password managers don't help

	Password Re-used?
(Intercept)	-1.07 ***
Complexity Ranking	-0.04 **
Times entered into each website	0.18 ***
Uses a Password Manager	0.00
$R^2_{GLMM_C}$	0.32

	# Websites (non-university)
(Intercept)	0.87 ***
Complexity (rank)	-0.01
Frequency of Entry (per website)	0.00
Uses Password Manager	0.01
University Password	3.20 ***
R^2_{LMMc}	0.124

Additional Results

(See paper for details)

Incorrect passwords are frequently passwords to other sites

People accurately self-report password re-use (r=0.12)

Summary

People re-use passwords that they have to enter frequently

Potential Explanations

1) People pick a complex password, enter it frequently to memorize it, and then re-use it. [a]

[a] J. Bonneau and S. Schechter. "*Towards reliable storage of 56-bit secrets in human memory*." USENIX Security, 2014

Potential Explanations

1) People pick a complex password, enter it frequently to memorize it, and then re-use it. [a]

2) Organizations require complex passwords be entered frequently. Already memorized for re-use. [b]

[a] J. Bonneau and S. Schechter. "*Towards reliable storage of 56-bit secrets in human memory*." USENIX Security, 2014

[b] D. Florêncio and C. Herley. "*Where Do Security Policies Come From?*" SOUPS, 2010

Don't use your MSU NetID and password for non-MSU accounts.

Passwords

Protect your NetID and password combination. Don't use your MSU NetID and password for social media sites, retail sites, or any non-MSU sites.

Reputable organizations will **NEVER** ask for your account and password combination in an email message.

Passphrase example

Even if your system does not support the length of a passphrase, a sentence can be the basis of a strong password.