

Password



Weak



RUB



RUHR-UNIVERSITÄT BOCHUM

On the Usability and Security of Password-Based User Authentication

Maximilian Golla

Thesis Defense, Bochum, Germany, May 29, 2019

hgi

Horst Görtz Institut
für IT-Sicherheit

User Authentication

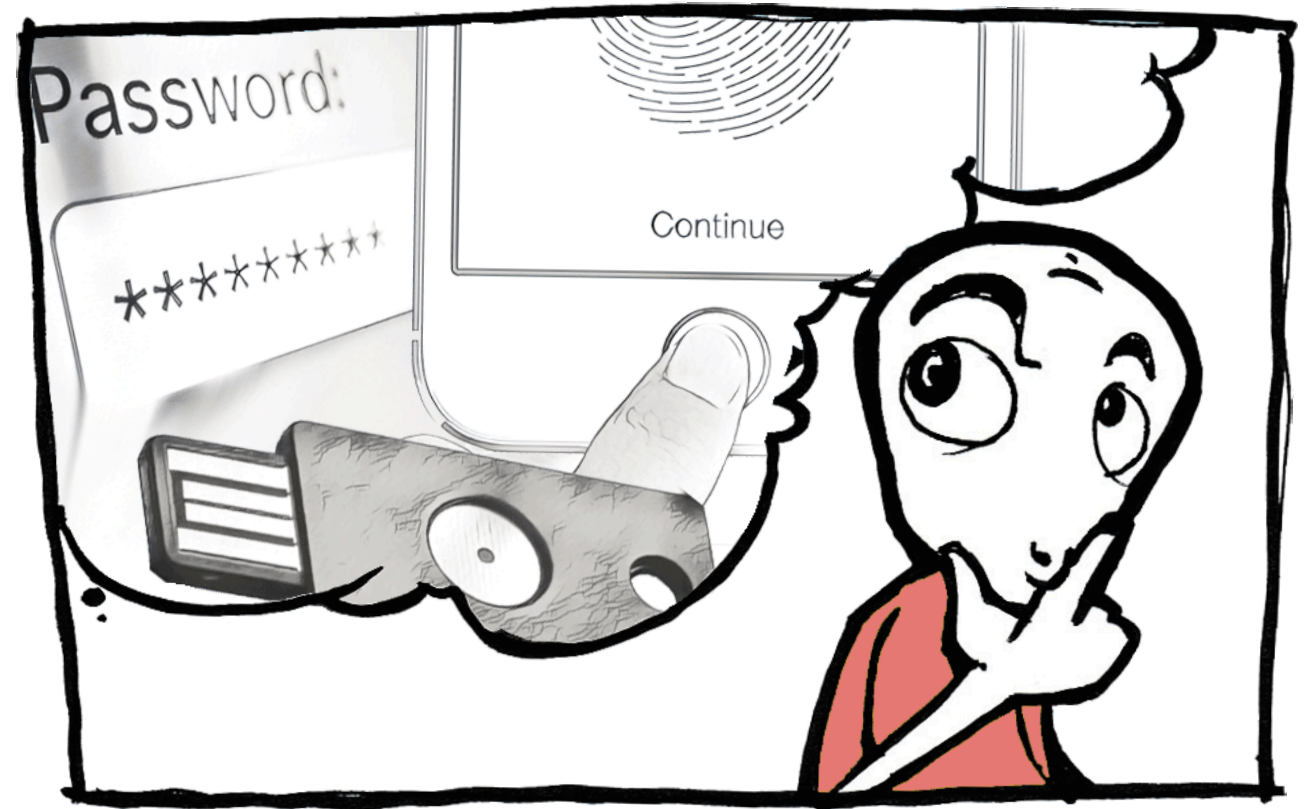
Competing requirements of **security** and **usability**.^[1]

Common Factors:

- ***🔒 Knowledge (**Password**, PIN)
- 👉 Biometrics (Fingerprint, Face)
- 🔑 Possession (Security Key)

Reinforced by:

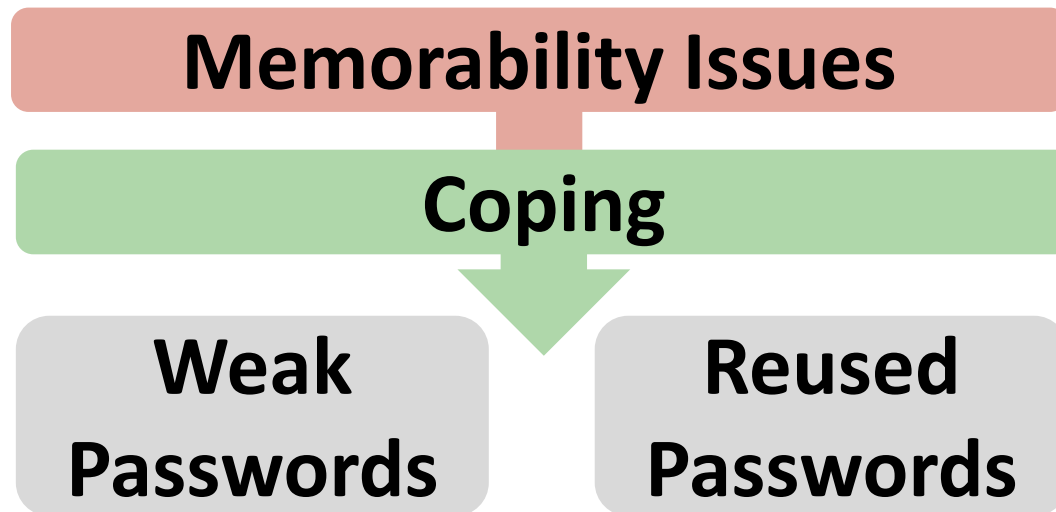
- 🔑 2-Factor Authentication
- 👤 Risk-based Authentication



Passwords Are Not Dead

Primary means of authentication on the Web. [2]

- Accounts: ~24
- Passwords: 6-8



Overview

Thesis



**Password
Management**

CCS 16



**Password
Strength**

CCS 18, SP 19



**Mobile
Authentication**

USEC 17, USEC 19, CCS 19*



**Password
Recovery**

PW 15, NDSS 17, USEC 19



**Password
Reuse**

CCS 18

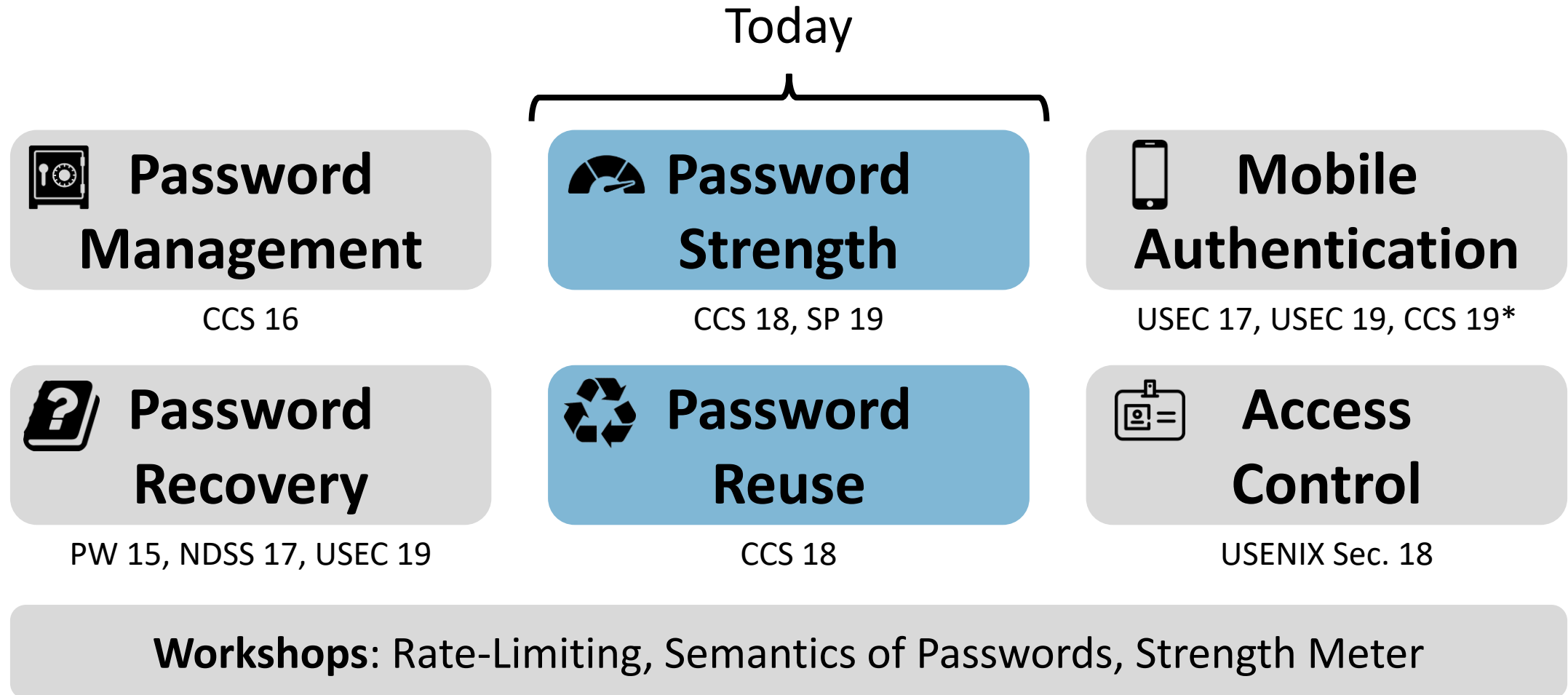


**Access
Control**

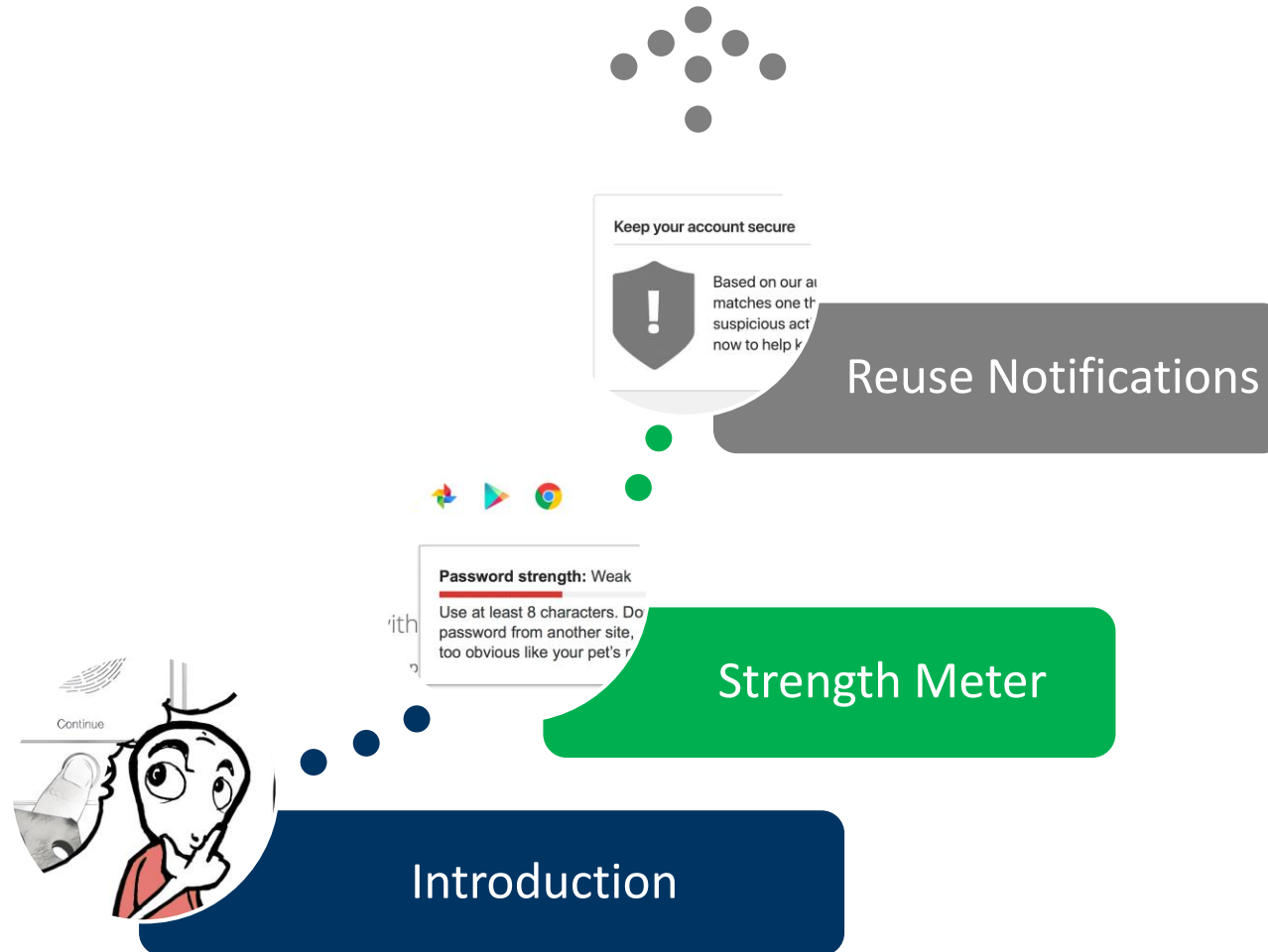
USENIX Sec. 18

Workshops: Rate-Limiting, Semantics of Passwords, Strength Meter

Overview



Outline



How Users Choose Passwords

- Well-defined process
- Misconceptions in mental model
 - “Adding ‘!’ to the end instantly makes it secure.” [3]
- Estimating strength not easy



Estimating the Strength of a Password is Tough

“Adding ‘!’ to the end instantly makes it secure.” [3]

Password 1:

iloveyou88

Password 2:

ieatkale88

Options:

- A. Password 1 is stronger
- B. Password 2 is stronger
- C. They are equally strong



Estimating the Strength of a Password is Tough

“Adding ‘!’ to the end instantly makes it secure.” [3]

Password 1:

iloveyou88

Guess Number:

1.5×10^4



Password 2:

ieatkale88

Guess Number:

3.1×10^9



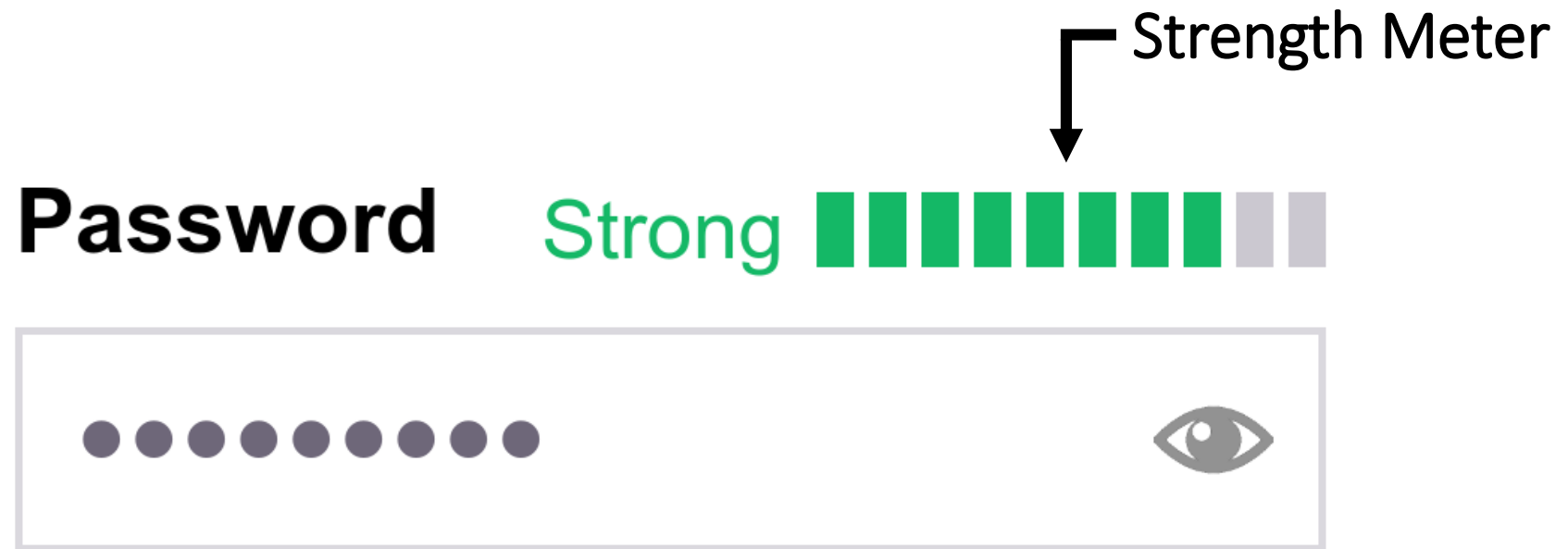
Guess Number

/ɡɛs ˈnʌmbə/

noun

1. The number of guesses required to guess a password.

Support Users in Choosing Secure Passwords



But They Are Not Always Accurate

Sign in Create an Account

An account is needed to access all of your Norton products and services.

g2963487@nwytg.com ?

g2963487@nwytg.com

Password123! | ?

First ?

Strength: Strong

- ✓ Use upper and lower case letters
- ✓ Use at least 1 number
- ✓ Use at least 1 symbol

Create Account

Sign in Create an Account

An account is needed to access all of your Norton products and services.

g2963487@nwytg.com ?

g2963487@nwytg.com

geyps5aykj0q71c637n9gf4ycg | ?

First ?

Strength: Weak

- ✗ Use upper and lower case letters
- ✓ Use at least 1 number
- ✗ Use at least 1 symbol

Create Account

How to Measure Accuracy?

Reference

Top	Count	Password
1	1 044 164	123456
2	176 120	password
...
1000	45 682	Baseball1

1 
2 
3 
Ranking



Strength Meter

Password  **Weak** 

123456 

1 
2 
3 
Ranking

Security and Login

https://www.facebook.com/settings?tab=security§ion=password&view

Chrome is being controlled by automated test software.

Search

Strength Home Find Friends Create

Notifications
Mobile
Public Posts
Apps and Websites
Instant Games
Business Integrations
Ads
Payments
Support Inbox
Videos

LUDS-based Meter:

Strong Password1

L: ✓ U: ✓ D: ✓ S: ✗

Login

Change password

It's a good idea to use a strong password that you're not using elsewhere

Current

New

Password strength: Weak


Re-type new

Forgot your password?

Save Changes

Terminal

```
Weak linkedin
Weak password
Weak 111111
Weak sunshine
Weak michael
Weak abduallah
Weak 666666
Medium 123456789
Medium 12345678
Weak thiago
Weak superman
Weak samson
Weak sammy1
Weak sailing
Strong Password1
Weak myaccount
Weak murphy
```



Password “Strength”

Meter	Example
Text	Weak, Medium, Strong
Colors	Red, Orange, Green
Percentages	42%
Scores	1-5
Time	12 d, 9h, 47m
Entropy	82 bits
Guess number	1 018 291 guesses

Reference: Guess number
Meter: ???



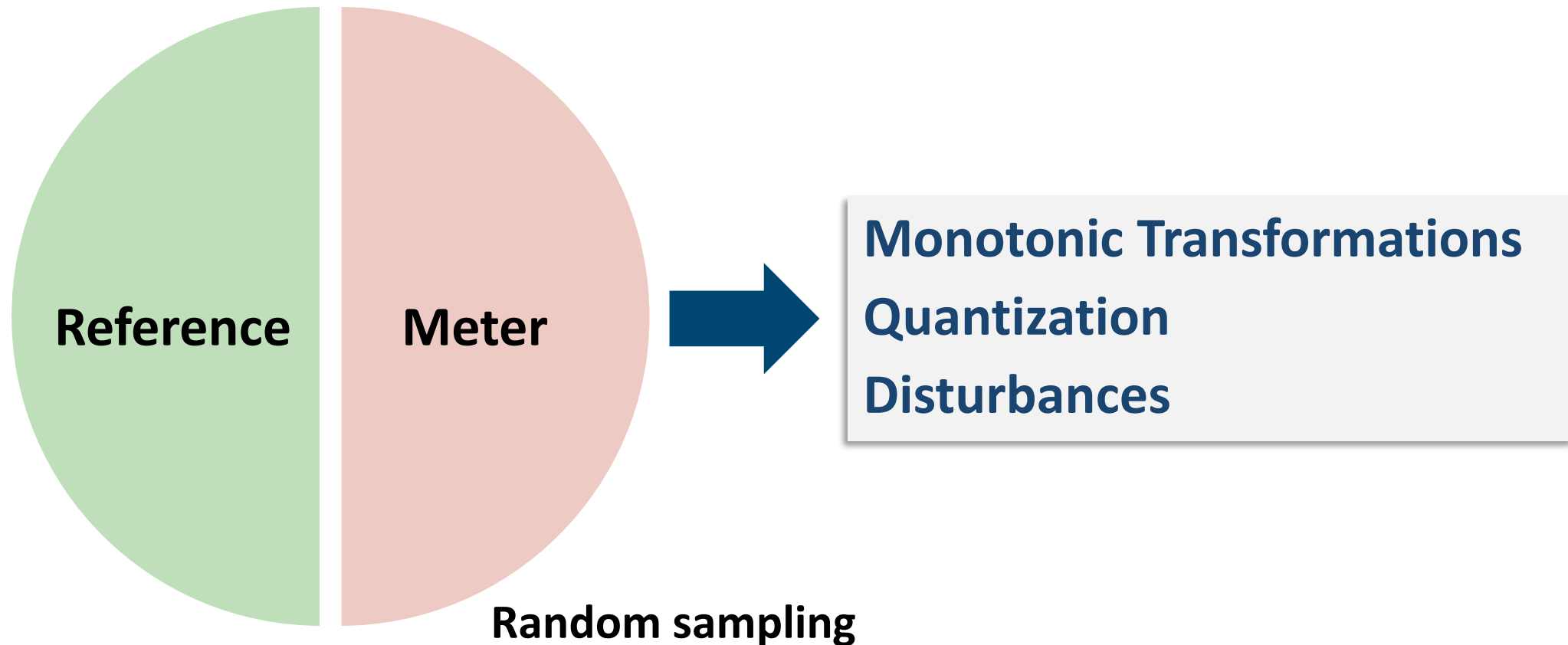
Simulation Dataset



Linked Passwords

Count	Password
1 044 164	123456
176 120	password
88 076	12345678
78 720	111111
...	...
356	charlie22
356	mickey7
...	...
1	~!@#!?~!@

Simulate Common Errors Observed in Real-World Meters



After: Quantized Output

Reference	Meter
63	40
19	30
9	20
3	20
2	10
1	10
...	...
(Count)	(Bin)



Result: Compare Weighted Ranking

4

Recommendation:

- Compare relative ranking only
- Weight passwords by importance

➔ Weighted and ranked metrics
(e.g., weighted Spearman correlation)

What can we do with this information?

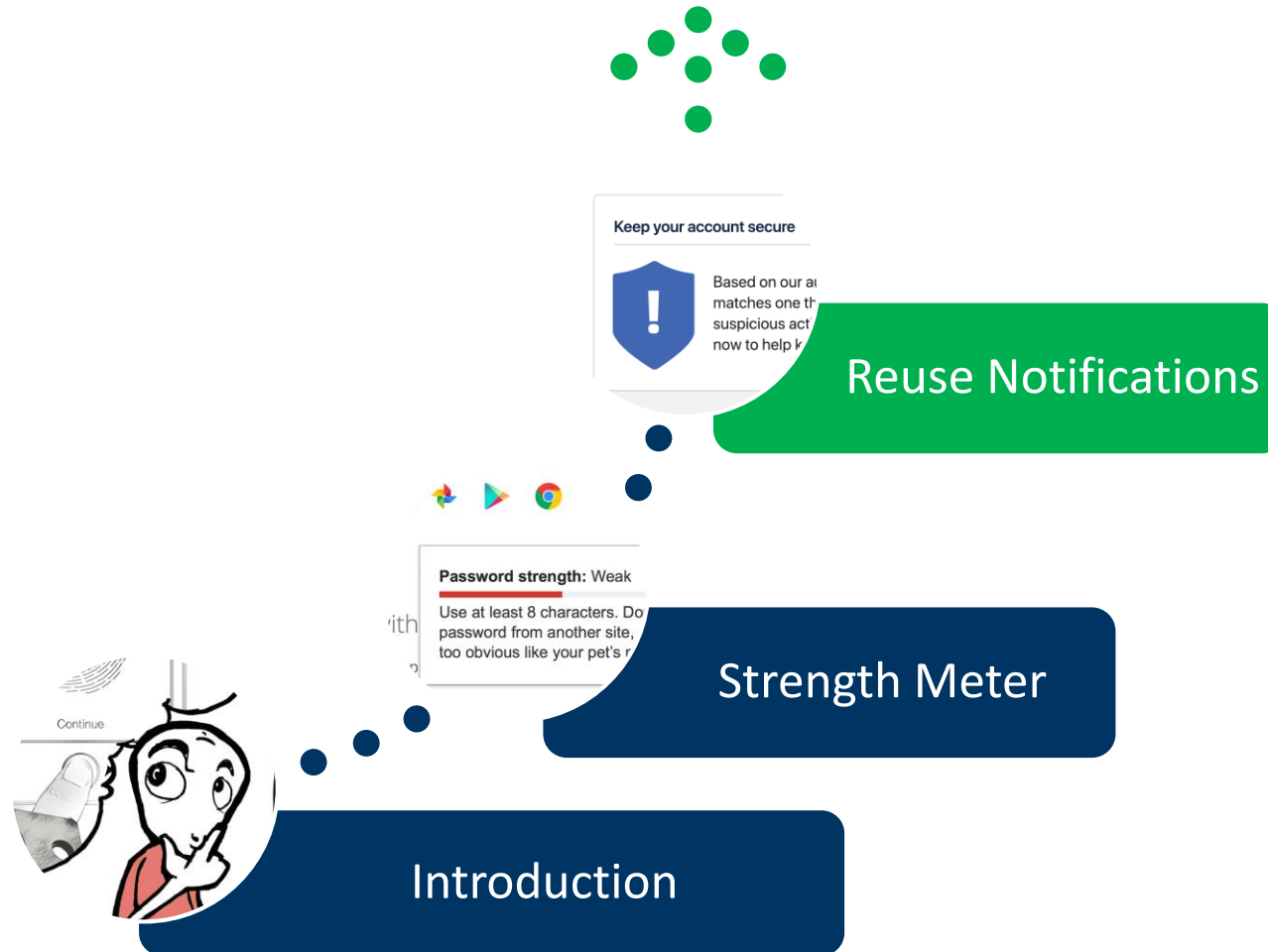
Large-Scale Comparison 81 implementations

- Academia
- Websites
- PW Manager
- Operating Systems
- Previous Work



password-meter-comparison.org

Outline



SO, UH, THAT BILLION-ACCOUNT YAHOO BREACH WAS ACTUALLY 3 BILLION

Anatomy of a pa
Adobe's giant-size
blur

Facebook
Facebook says 14
had personal dat
recent breach

Hackers were able to access name, bir
nearly half of the 30 million accounts

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

RISK ASSESSMENT —

How LinkedIn's password sloppiness

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address pwned?

364
pwned websites

7,858,347,021
pwned accounts

95,745
pastes

117,180,866
paste accounts

tracking future dumps.

theguardian

Q f t r y



facebook

Email or Phone Password

Sign Up

Connect with friends and the

You Can Now Look Up Your Terrible 2006 MySpace Password

June 29, 2016 // 11:35 AM EST

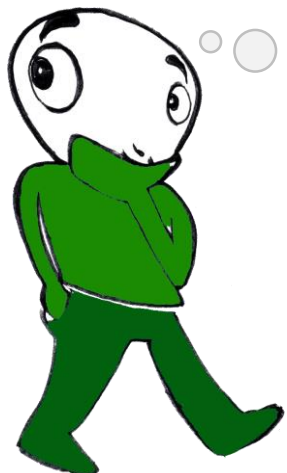


Written by
LORENZO FRANCESCHI-
BICCHIERI
STAFF WRITER

Reuse Attacks?

LinkedIn

Email	Cracked SHA-1
jenny@gmail.com	Hiking91
joe@mail.com	R0cky!17
john@hotmail.com	ILoveBananas!
...	...



I used
"R0cky!17"
everywhere!

1 guess can be enough!




AcmeCo

Email	Secure Argon2i Hash
joe@mail.com	\$argon2i\$v=19\$m=4096,...
...	...

Facebook buys black market passwords to keep your account safe

The company's security chief says account safety is about more than just building secure software.

BY KATIE COLLINS  | NOVEMBER 9, 2016 12:56 PM PST

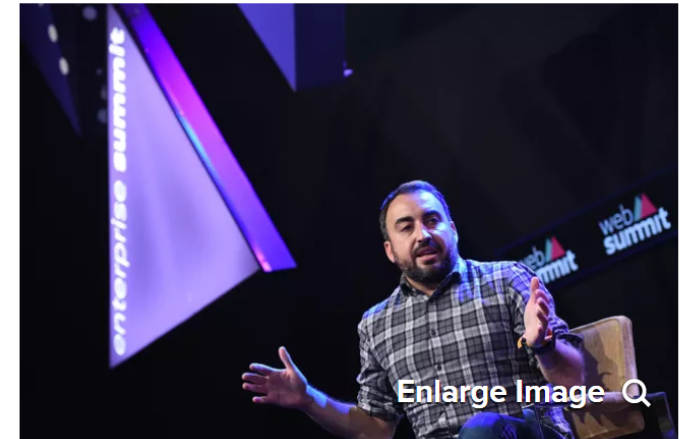


For a data-saturated company of its size and scope, Facebook has markedly managed to avoid the kind of security scandals, breaches and hacks that have affected many other major web companies.

Take a closer look, and you'll see why. Though on the surface all seems calm, below the waves the social network is kicking its legs frantically and working around the clock to keep users' accounts safe.

Keeping Facebook safe and keeping it secure are two different things, the social network's chief security officer, Alex Stamos, said Wednesday at Web Summit in Lisbon. Security is about building walls to keep out threats and shore up defenses, but according to Stamos, safety is bigger than that.

"It turns out that we can build perfectly secure software and yet people can still get hurt," he said.



"The reuse of passwords is the No. 1 cause of harm on the internet," says Facebook's Alex Stamos.

Brendan Moran/Getty Images

“Stolen From Another Site”

Keep your account secure



Based on our automated security check, your Facebook password matches one that was stolen from another site. We aren't aware of any suspicious activity on your account, but please change your password now to help keep it secure.

[Learn More](#)[Continue](#)

Study 1: Previously Sent Notifications



Understanding



Feelings



Actions



Perceptions

Effectiveness

Delivery Method

Legitimacy

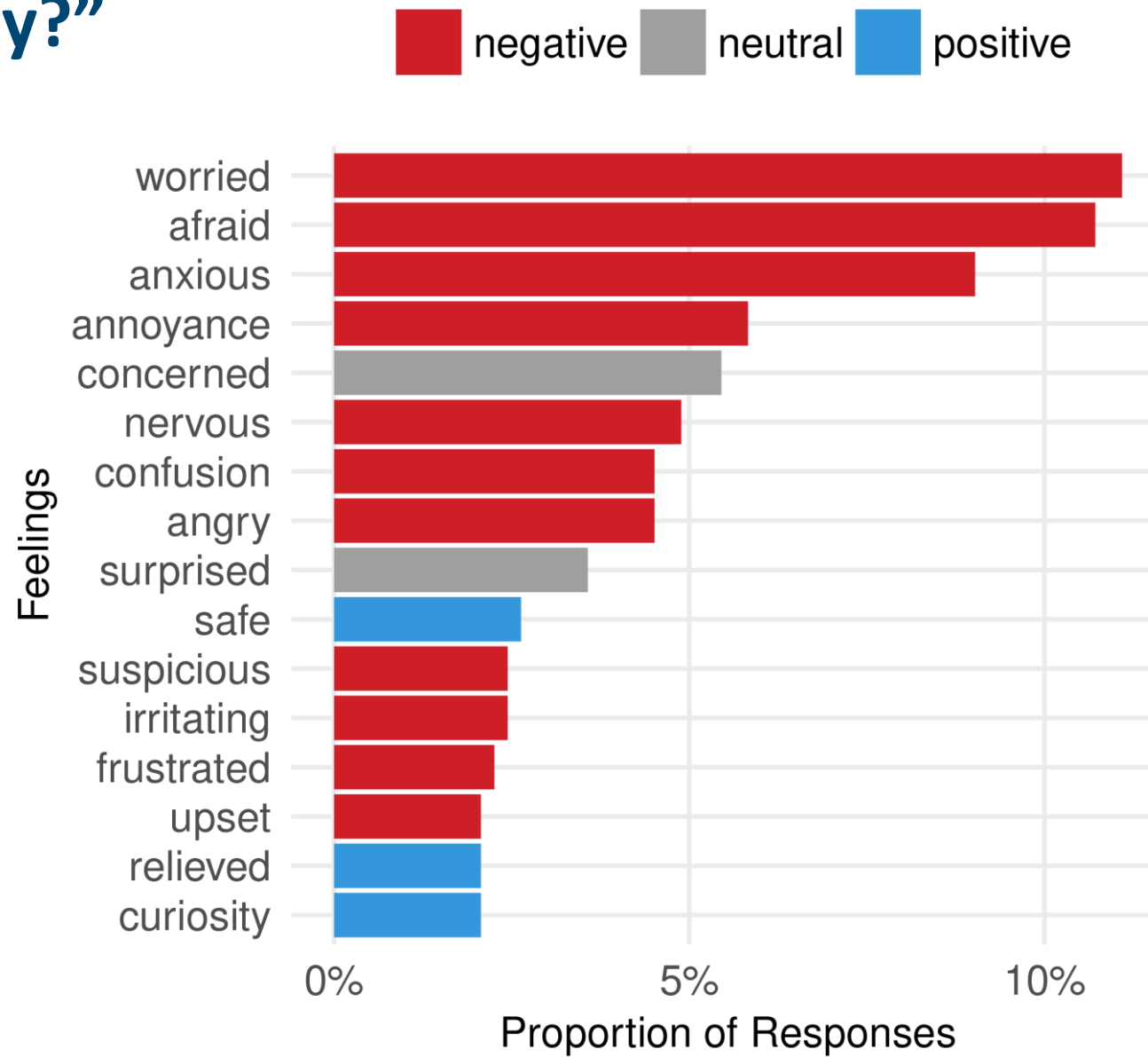


MTurk, 15min, 180 respondents, \$2.50

“You've got e-mail! ... shall I deal with it now?”

 Concerning and a priority
(83% very high or high)

“Should I worry?”



“Something happened and you need to click ‘OK’ to get on with things.” [6]

What may have caused you to receive this notification?

[Multi select]

60% Account hacked

21% New device (false alarm)

21% Data breach

19% Reuse



Call a Spade a Spade!

Don't mention reuse



0 - 4%

respondents

Allude to reuse



48 - 56%

respondents

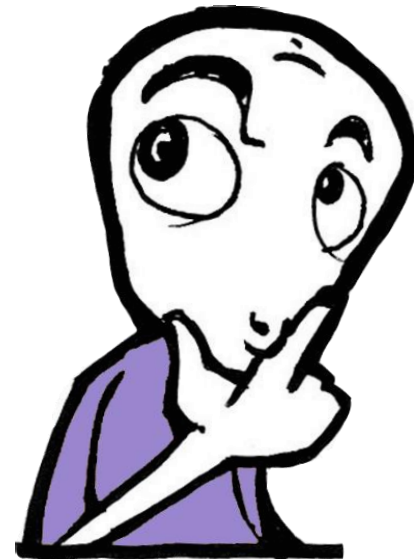
listed reuse as a cause
for receiving this notification.

Incomplete Mental Models

*“The chances of someone guessing that I use the same password are still incredibly low.”
(R171)*

Current password-reuse notifications:

- ✓ cause concern
- ✗ explain the situation



Study 2: Components of Notifications



Delivery Medium

Push / In-App / Email



Incident

Unrelated / Our / -



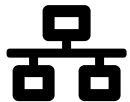
Account Activity

No suspicious / Suspicious / -



Remediation

Create new / Recommend



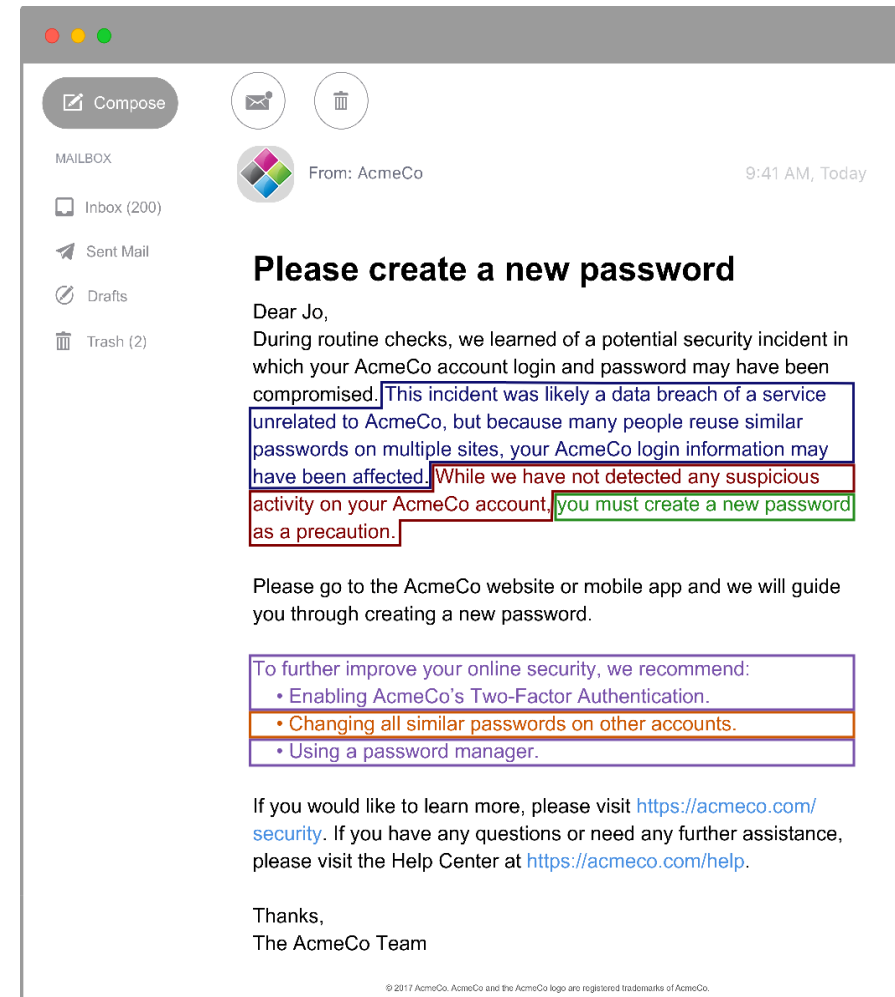
Other Accounts

Change all / -



Extra Actions

Enable 2FA + Manager / -



MTurk, 588 Respondents

... Unhealthy Behavior

What would you do about it?

90% Change it

6% Keep it the same

4% Don't know

What would your new password be?

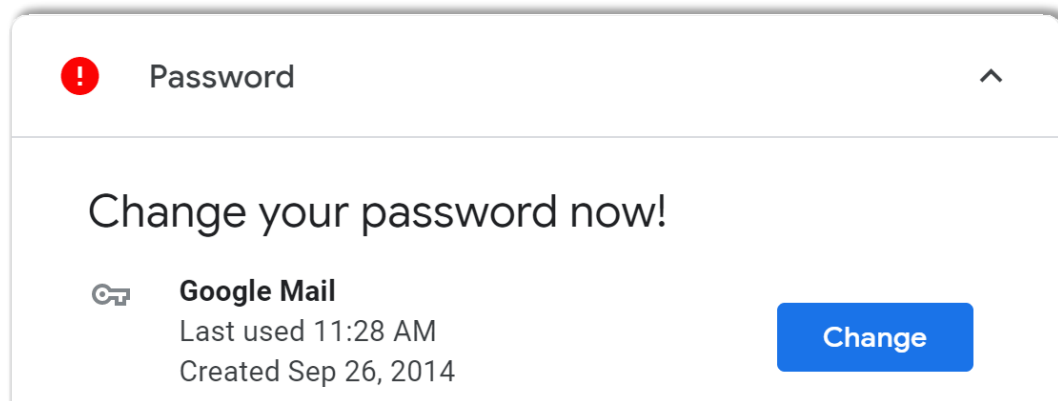
68% Modified password

13% Reused password

11% Use manager/browser

6% Other

2% Completely new

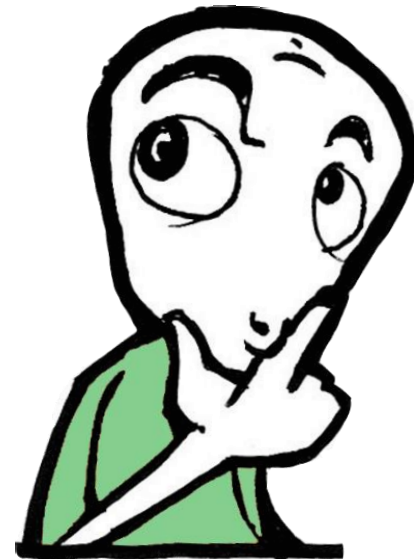


Incomplete Mental Models

*“The hack wasn't specific to this company so it
doesn't worry me.”
(R69)*

After seeing a reuse notification, users

- ✓ would change password
- ✗ ... but ineffectively
- ✗ have incomplete mental models



Mockup

Create your Google Account

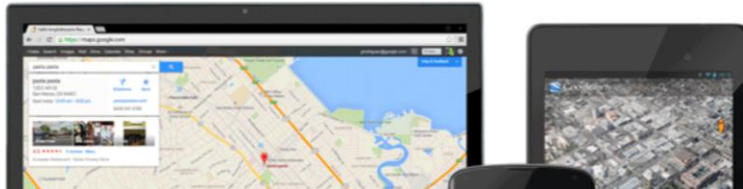
One account is all you need

One free account gets you into everything Google.



Take it all with

Switch between devices, and pick up



Password strength: Weak

Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. [Why?](#)

Name

First

Last

Choose your username

@gmail.com

Create a password

.....



Safari detected that you are **reusing a password.**

Consider using this **strong password instead.**

funrus-Hommez-kajzo7

This password will be saved to your iCloud Keychain and will AutoFill on all your devices. Look up your saved passwords in Safari Passwords preferences or by asking Siri.

Gender

Conclusion

