

# Password



Weak



RUHR-UNIVERSITÄT BOCHUM

## On the Usability and Security of Password-Based User Authentication

Maximilian Golla

Thesis Defense, Bochum, Germany, May 29, 2019

# User Authentication

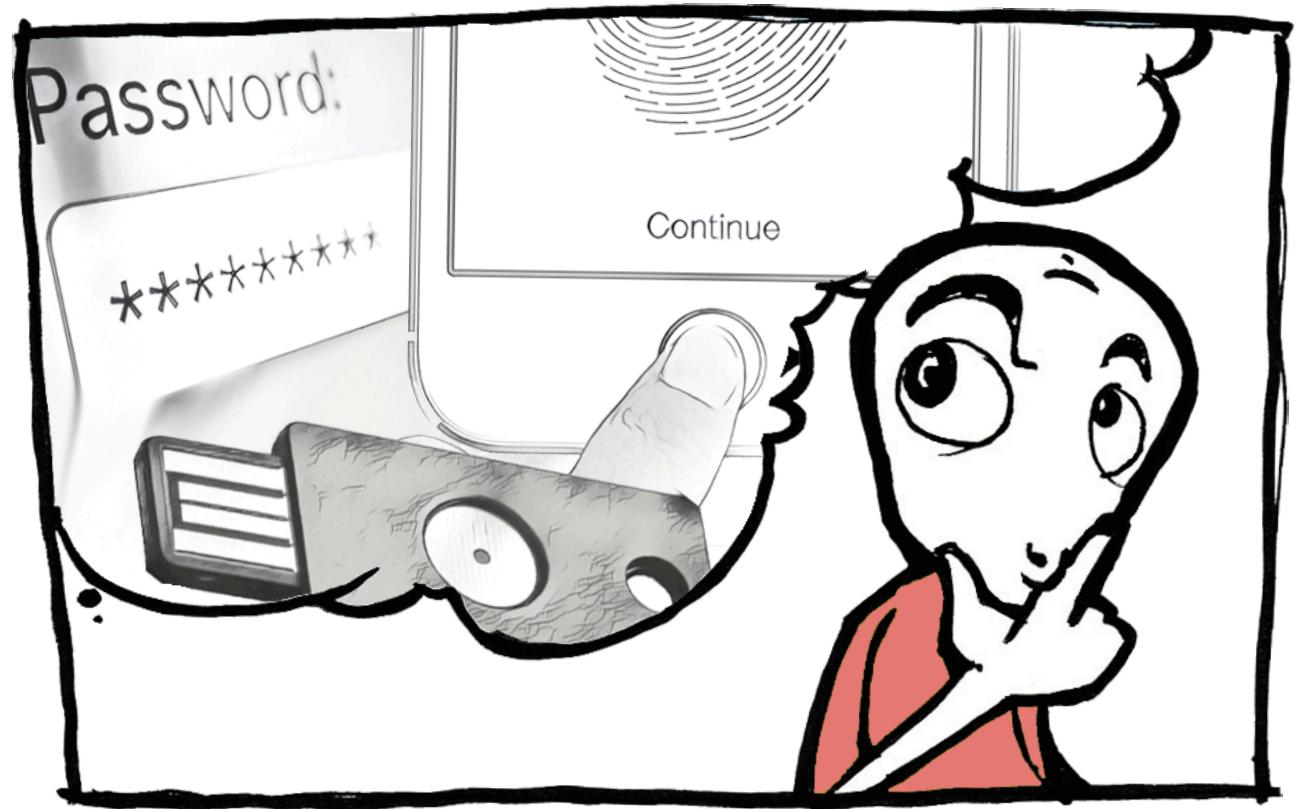
Competing requirements of **security** and **usability**. [1]

## Common Factors:

- >Password (PIN)
- Fingerprint, Face
- Security Key

## Reinforced by:

- 2-Factor Authentication
- Risk-based Authentication

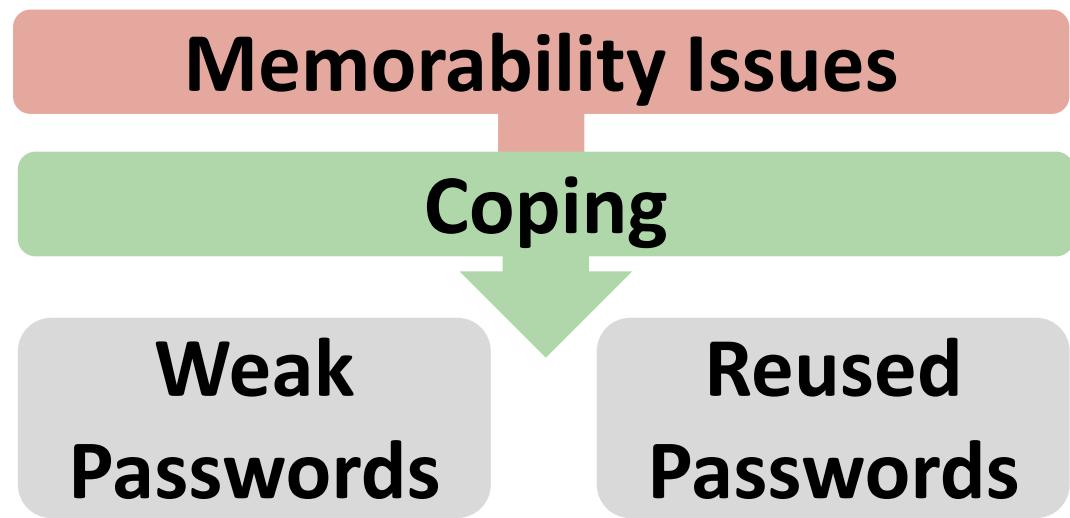


<sup>3</sup> [Ref. 1] Joseph Bonneau et al.: **The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes.** (SP '12)

# 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

Today



## Password Management

CCS 16



## Password Recovery

PW 15, NDSS 17, USEC 19



## Password Strength

CCS 18, SP 19



## Password Reuse

CCS 18



## Mobile Authentication

USEC 17, USEC 19, CCS 19\*

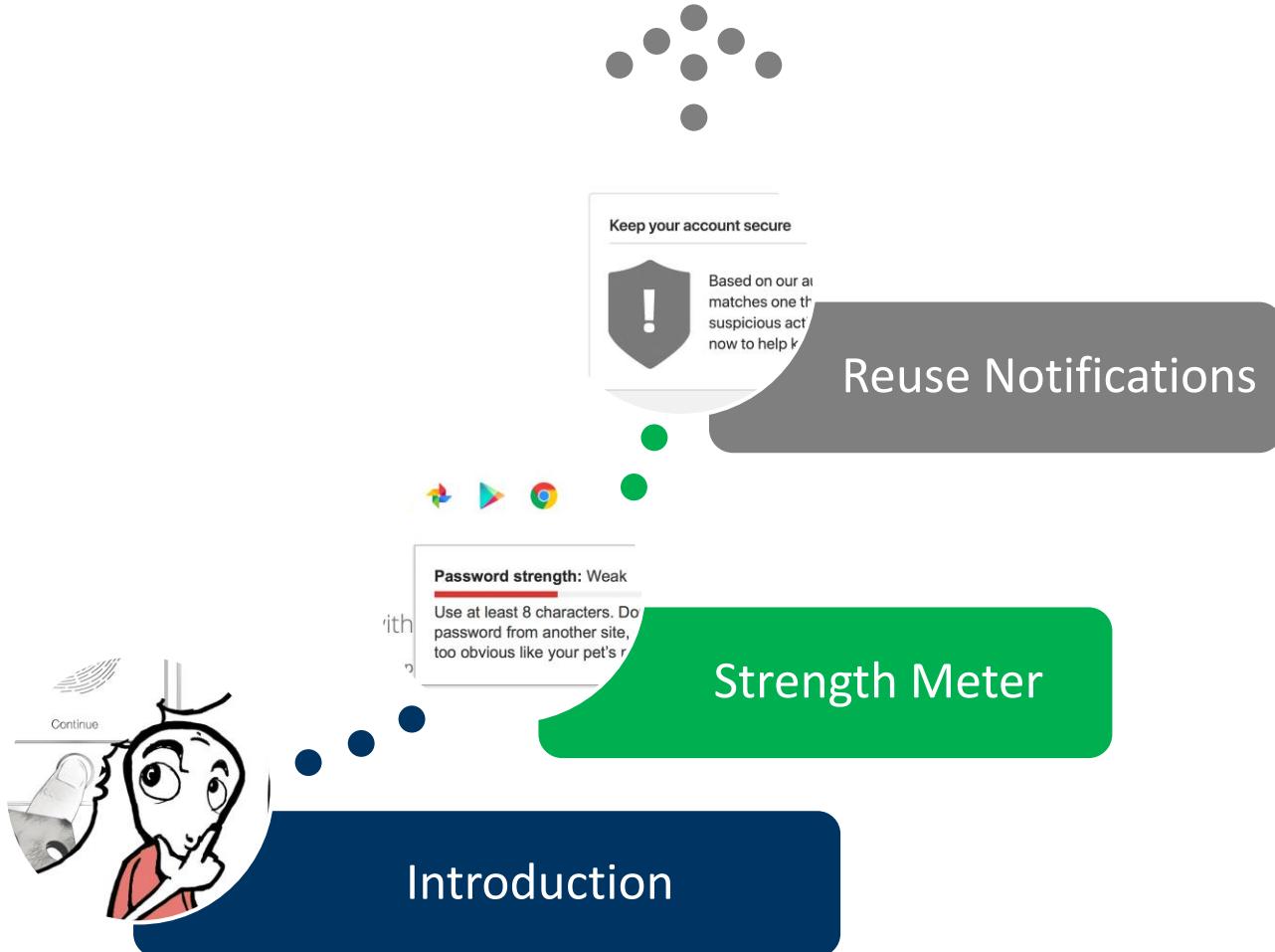


## Access Control

USENIX Sec. 18

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

# 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:

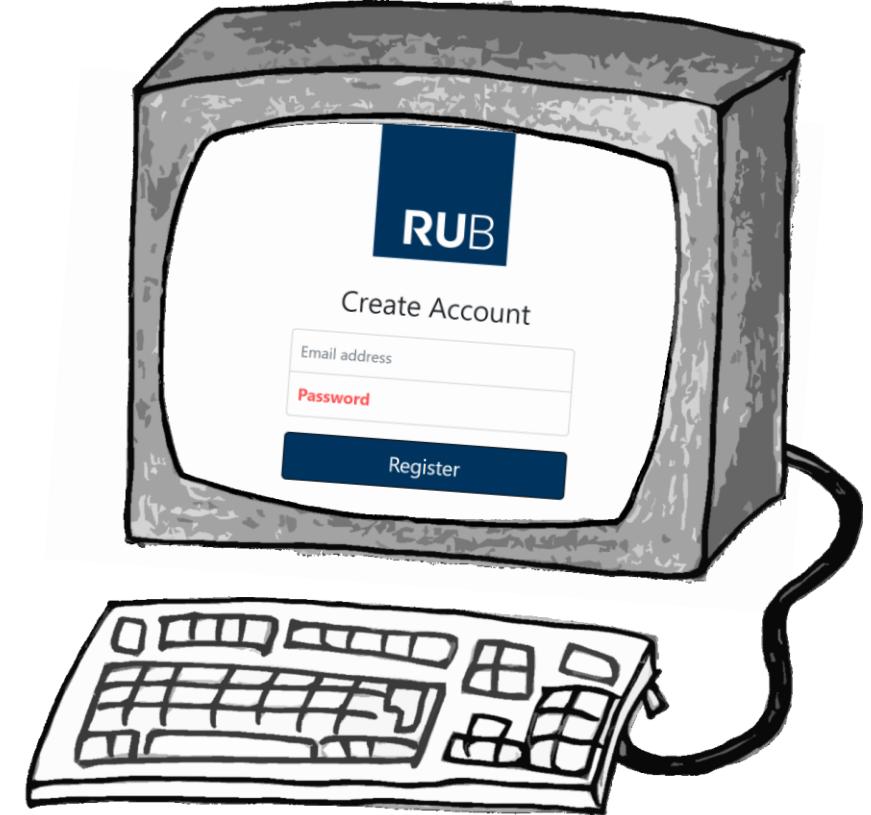
iloveyou88

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:

**$1.5 \times 10^4$**

Password 2:

ieatkale88

Guess Number:

**$3.1 \times 10^9$**



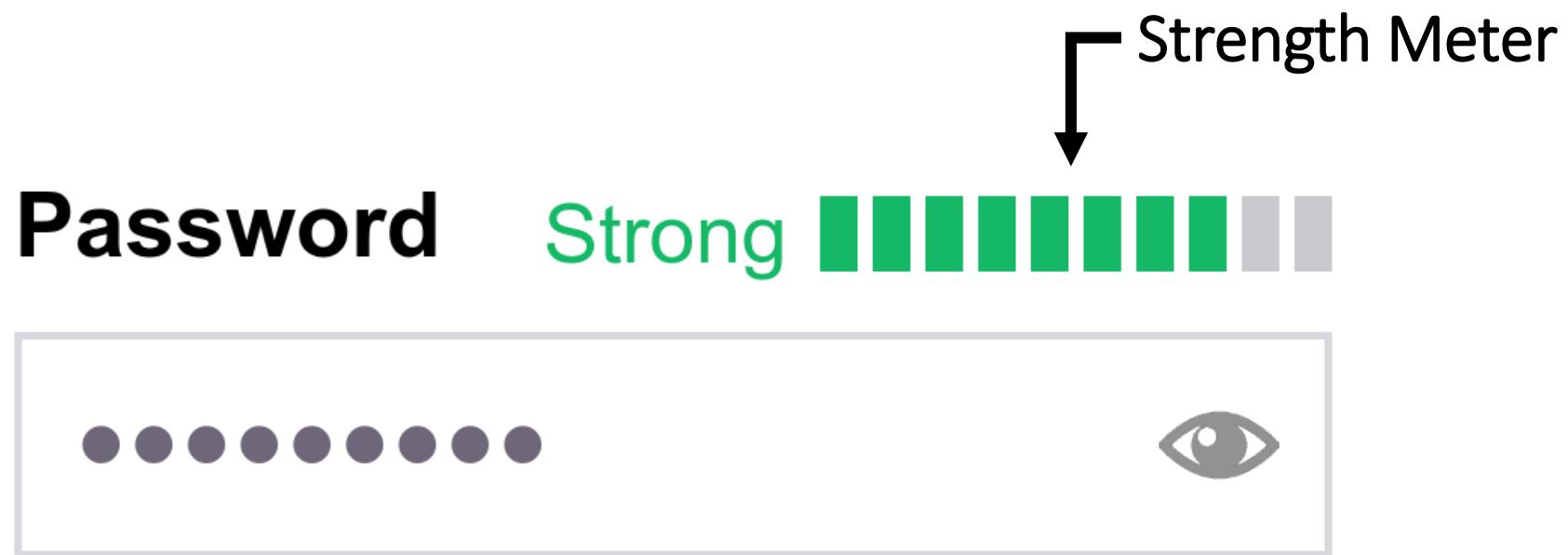
**Guess Number**

/ges 'nʌmbə/

*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.

?

?

?

?

?

Your password must be 6 characters or longer.  
For a more secure password:

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

**Strength:** Strong

**Create Account**

Sign in      Create an Account

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

?

?

?

?

?

Your password must be 6 characters or longer.  
For a more secure password:

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

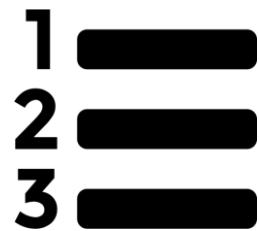
**Strength:** Weak

**Create Account**

# How to Measure Accuracy?

## Reference

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



Ranking

## Strength Meter



Ranking

Security and Login x + https://www.facebook.com/settings?tab=security&section=password&view

Chrome is being controlled by automated test software.

Search Strength Home Find Friends Create

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

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



Bochum, May 29, 2019 | Thesis Defense '19

RUB

# 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: ???



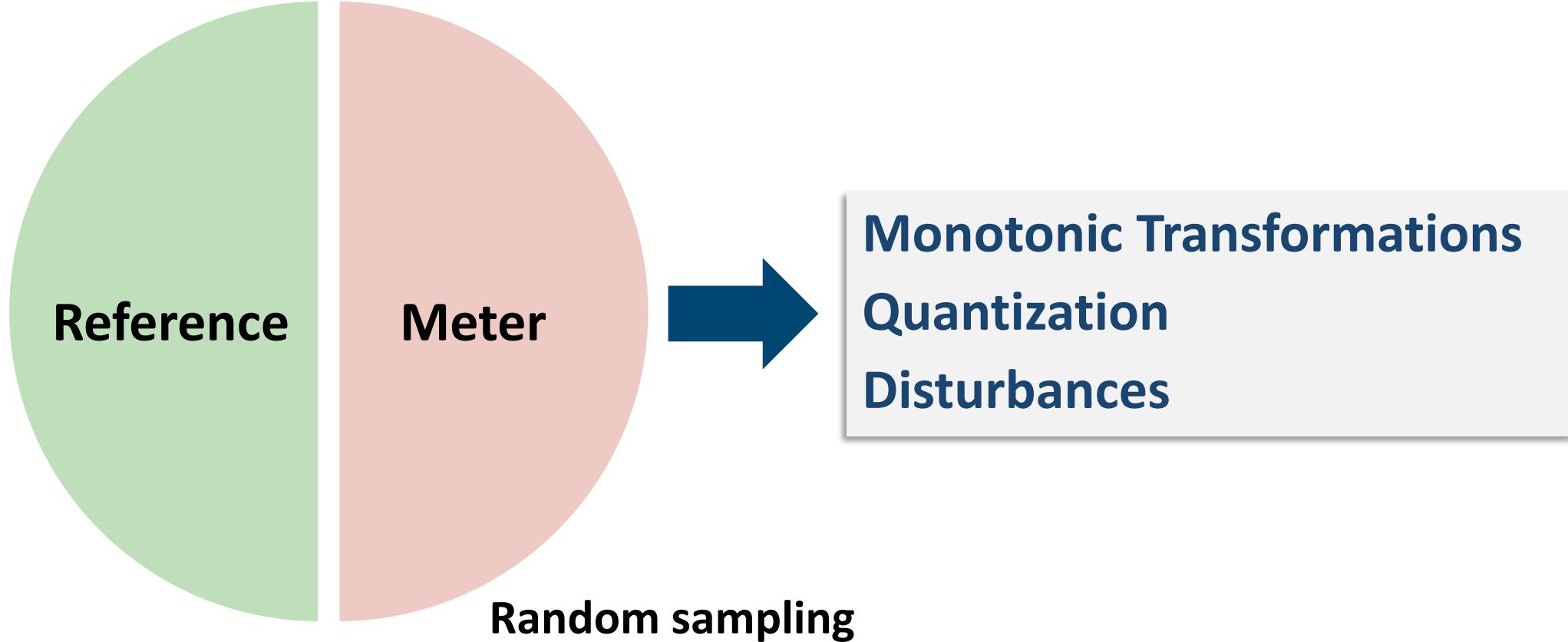
# Simulation Dataset



**LinkedIn 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

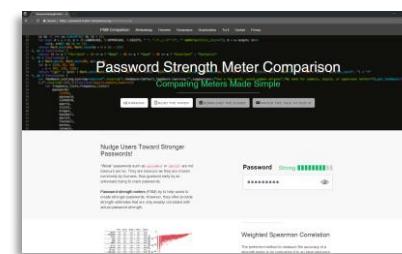
## Recommendation:

- Compare relative ranking only
  - Weight passwords by importance
- ➡ Weighted and ranked metrics  
(e.g., weighted Spearman correlation)

## Large-Scale Comparison 81 implementations

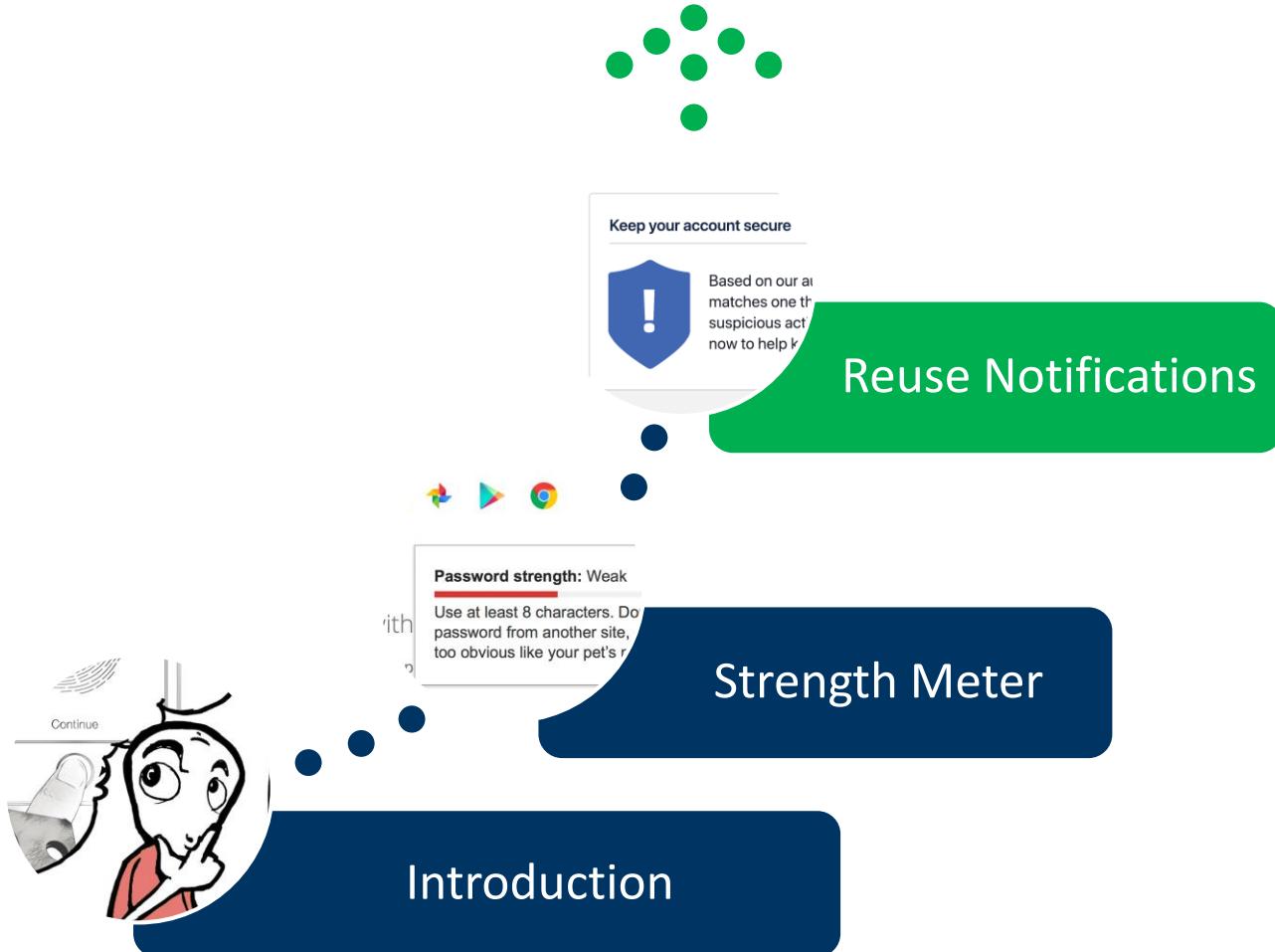
- Academia
- Websites
- PW Manager
- Operating Systems
- Previous Work

What can we do with this information?



[password-meter-comparison.org](http://password-meter-comparison.org)

# Outline



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

Anatomy of a password breach  
Adobe's giant-size password dump  
blurred lines

Facebook

Facebook says 123 million users had personal data exposed in recent breach

Hackers were able to access name, birth date, and email address for 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	7,858,347,021	95,745	117,180,866
pwned websites	pwned accounts	pastes	paste accounts

You Can Now Look Up Your Terrible 2006 MySpace Password

June 29, 2016 // 11:35 AM EST

Written by LORENZO FRANCESCHI-BICCHERAI STAFF WRITER

Bochum, May 29, 2019 | Thesis Defense '19

**RUB**

# Reuse Attacks?

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



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

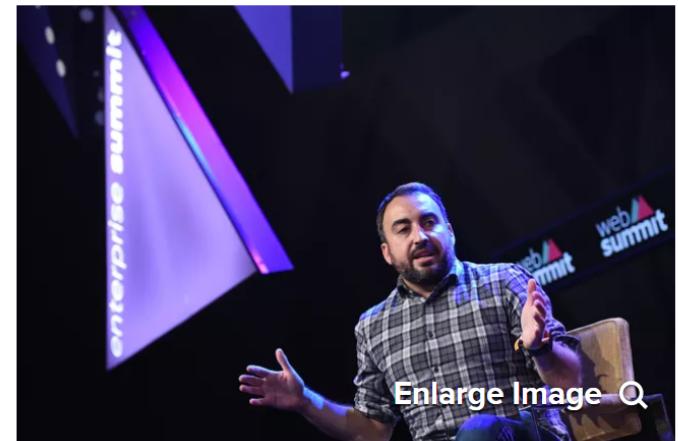


For a data-saturated company of its size and scope, Facebook has markedly managed to avoid the kind of security scandals, breaches and hacks that have affected many other major web companies.

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

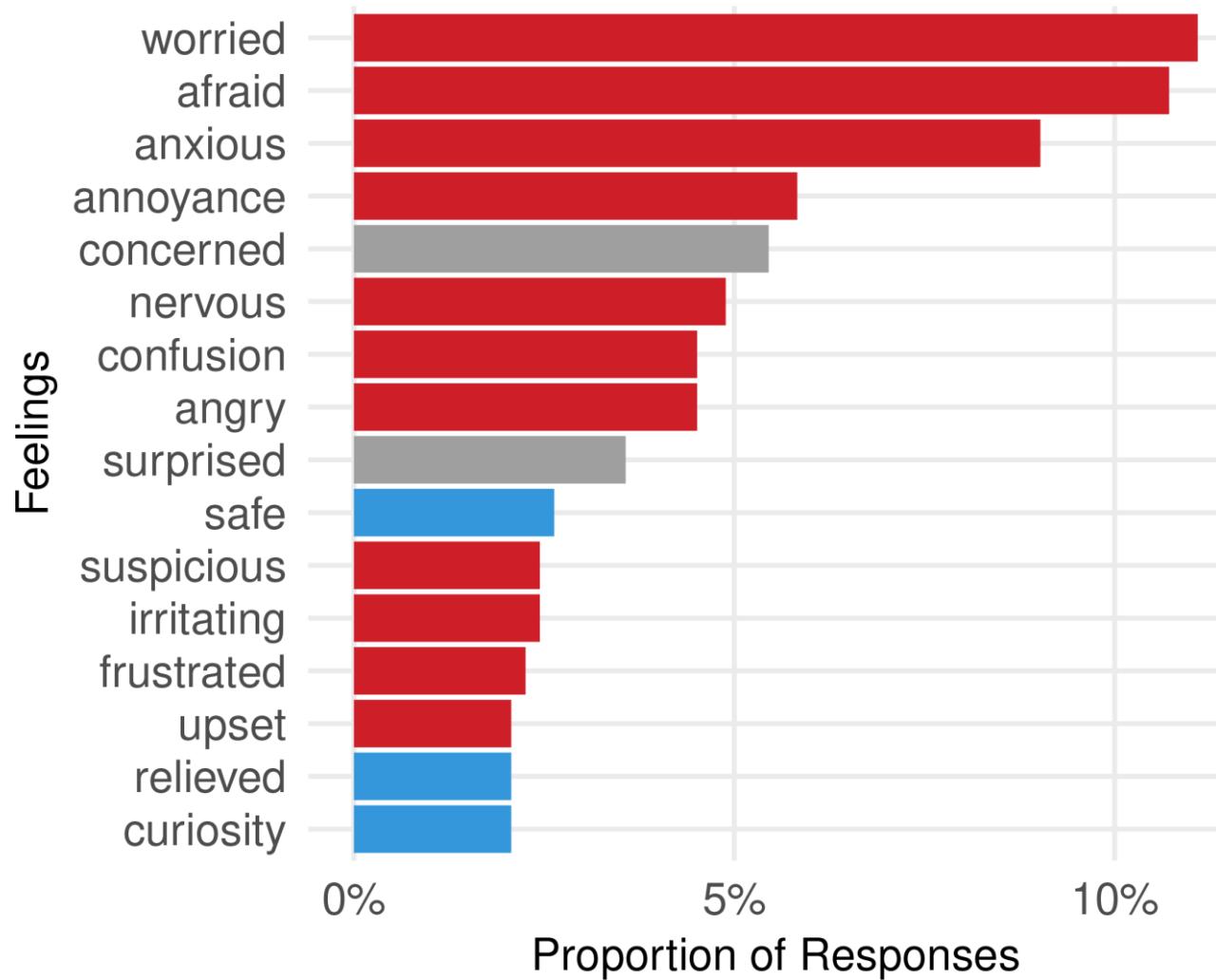
# “You've got e-mail! ... shall I deal with it now?”



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

# “Should I worry?”

negative neutral positive



# “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)

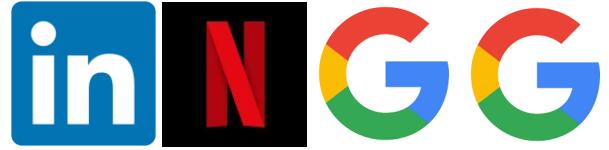
21% Data breach

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.

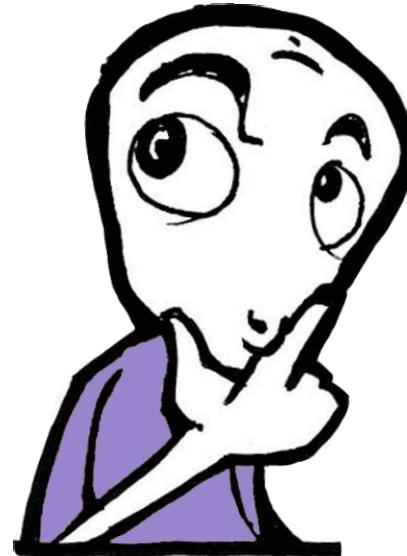
# Incomplete Mental Models

*“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 / -



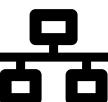
## Account Activity

No suspicious / Suspicious / -



## Remediation

Create new / Recommend



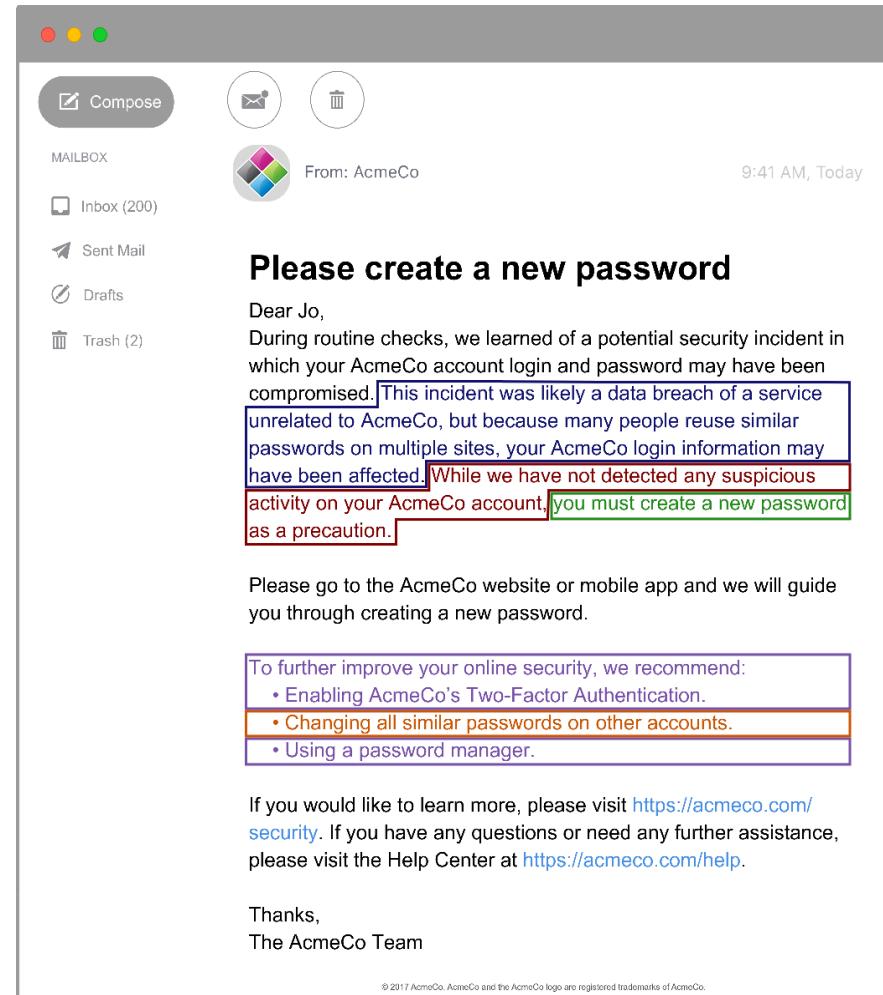
## Other Accounts

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?*

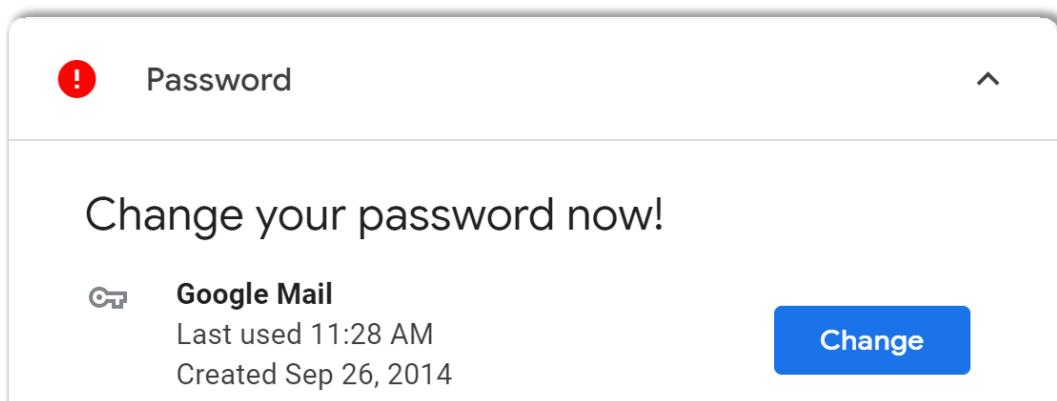
68% Modified password

13% Reused password

11% Use manager/browser

6% Other

2% Completely new

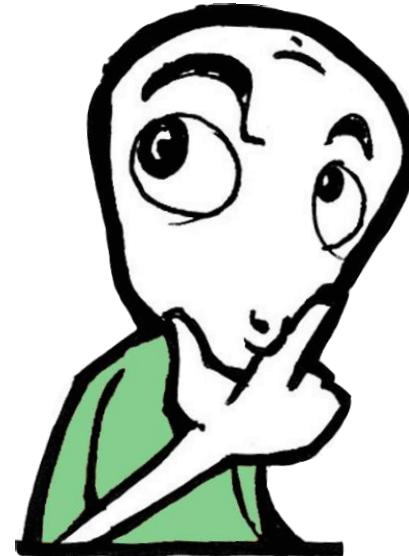


# Incomplete Mental Models

*“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



# Create your Google Account

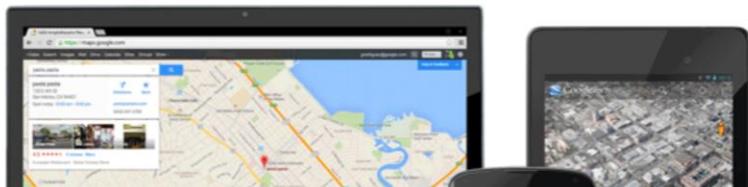
One account is all you need

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.

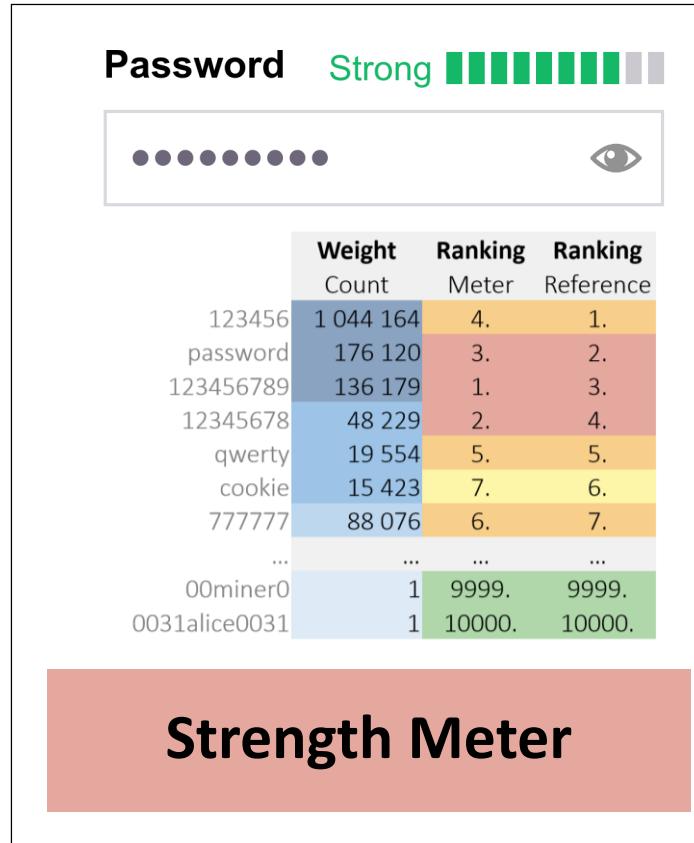
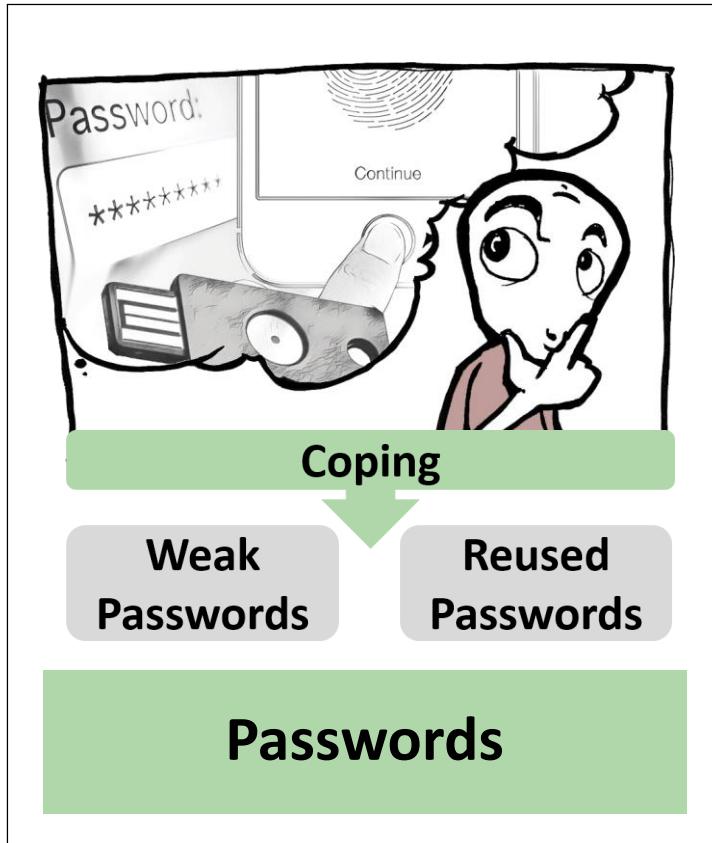
Consider using this **strong password** instead.

**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



**Please create a new password**

Dear Jo,

During routine checks, we learned of a potential security incident in which your AcmeCo account login and password may have been compromised. This incident was likely a data breach of a service unrelated to AcmeCo, but because many people reuse similar passwords on multiple sites, your AcmeCo login information may have been affected. While we have not detected any suspicious activity on your AcmeCo account, you must create a new password as a precaution.

Please go to the AcmeCo website or mobile app and we will guide you through creating a new password.

To further improve your online security, we recommend:

- Enabling AcmeCo's Two-Factor Authentication.
- Changing all similar passwords on other accounts.
- Using a password manager.

If you would like to learn more, please visit <https://acmeco.com/security>. If you have any questions or need further assistance, please visit the Help Center at <https://acmeco.com/help>.

Thanks,  
The AcmeCo Team

© 2017 AcmeCo. AcmeCo and the AcmeCo logo are registered trademarks of AcmeCo.

**Reuse Notifications**