"What was that site doing with my Facebook password?"

Designing Password-Reuse Notifications

Maximilian Golla
Miranda Wei
Juliette Hainline
Lydia Filipe
Markus Dürmuth
Elissa Redmiles
Blase Ur

THE UNIVERSITY OF CHICAGO

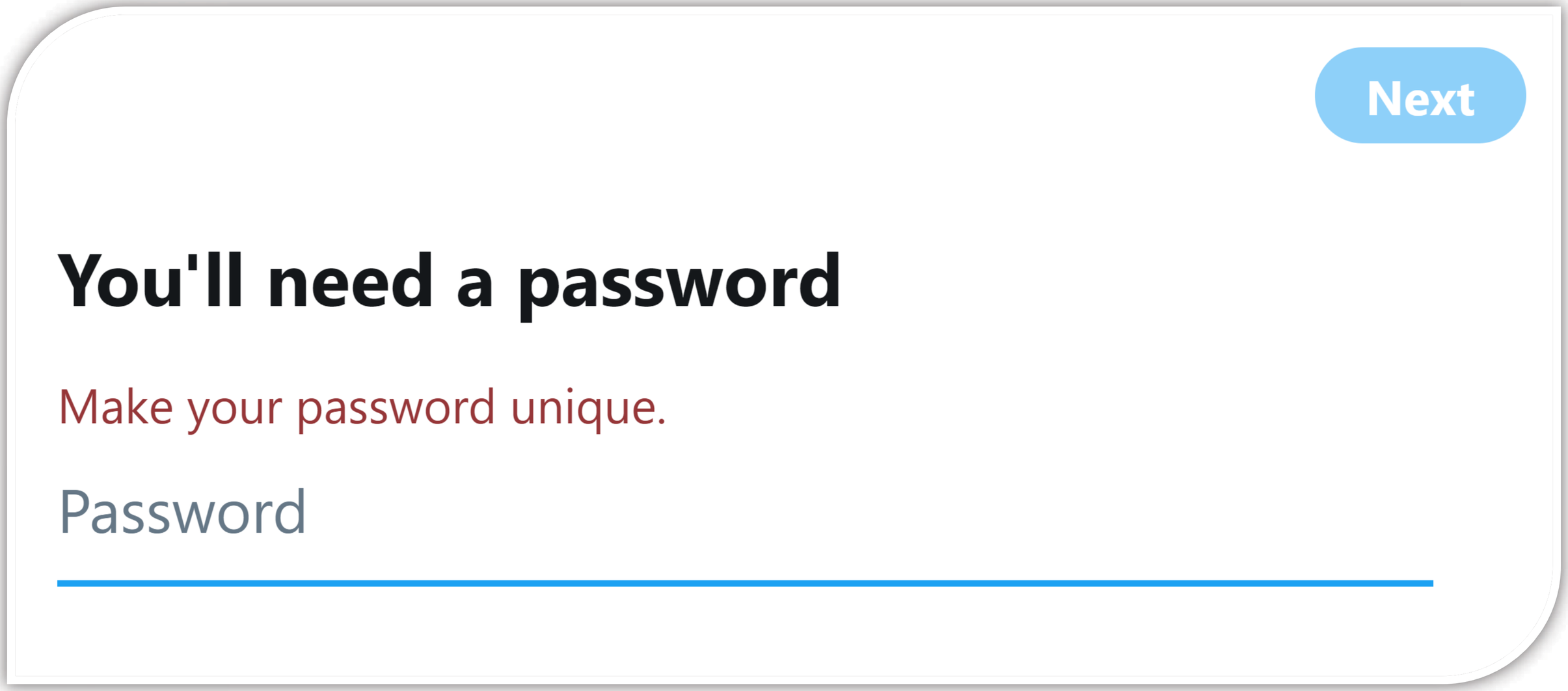
RUHR UNIVERSITÄT BOCHUM RUB

UNIVERSITY OF MARYLAND

UCHICAGO SUPER GROUP Security, Usability, & Privacy Education & Research

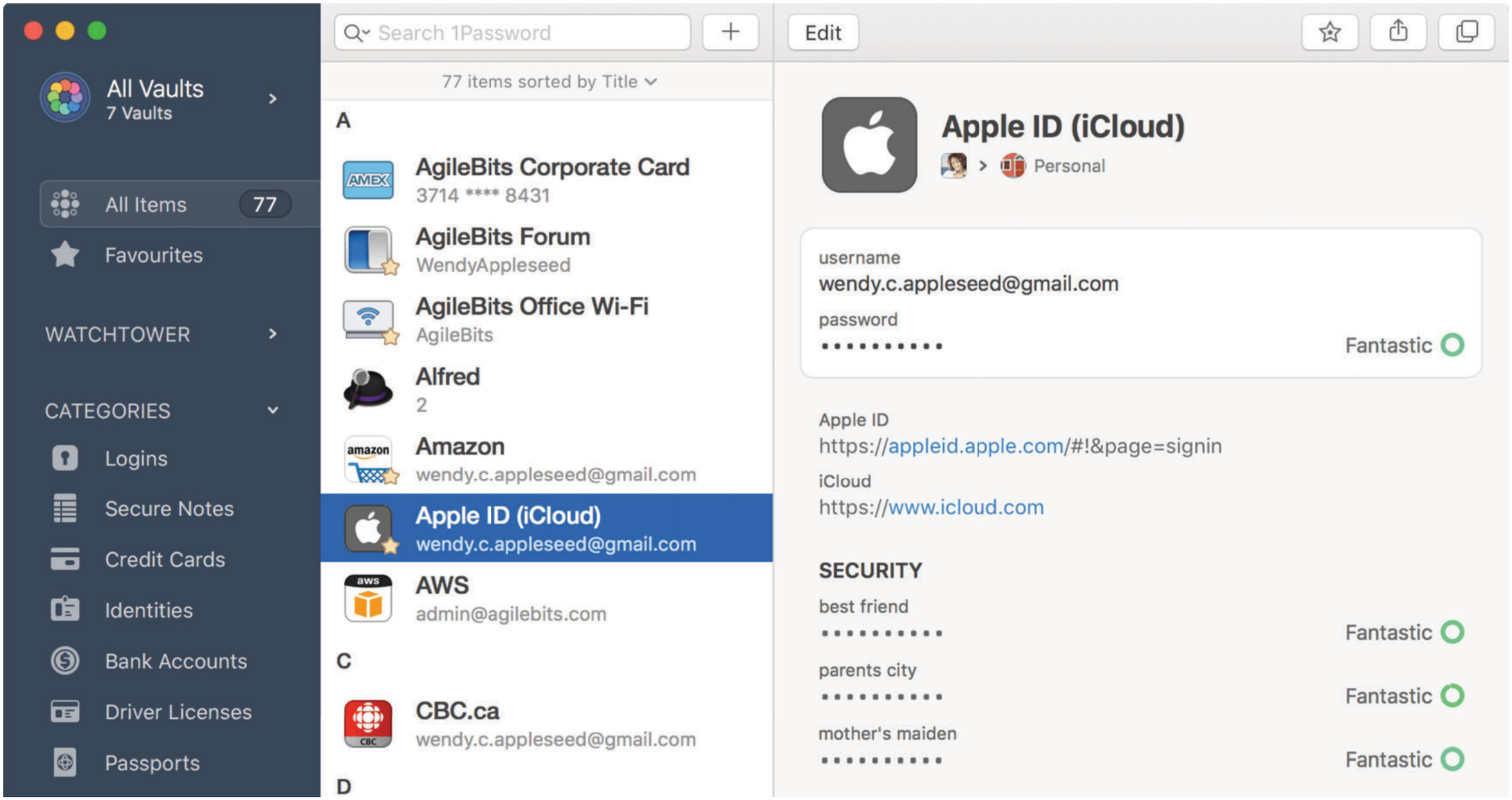
Toronto, Canada | ACM CCS | October 18, 2018

use unique passwords




Booking.com
Spotify
PayPal
American Airlines
reddit
Baidu 百度
WELLS FARGO
1&1
淘宝网
Taobao.com
Dropbox
airbnb
facebook
twitter
Adobe
ebay
YouTube
Microsoft
slack
SONY
Google

“use a password manager!”



people reuse passwords

R0cky!14

R0cky!17

R0ckyBox

R0cky!17

R0cky!17

123456

R0ckyStar

Rocky!16

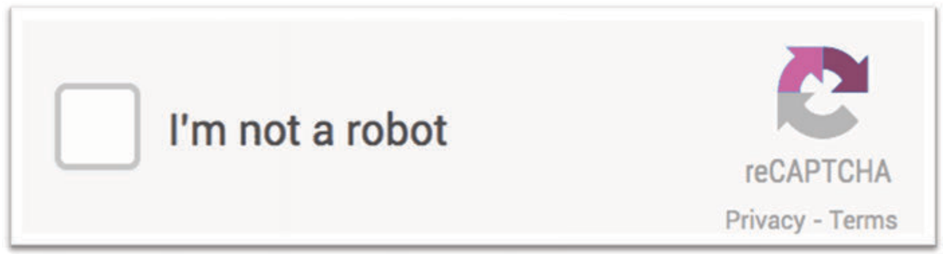
R0cky!17

AcmeCo

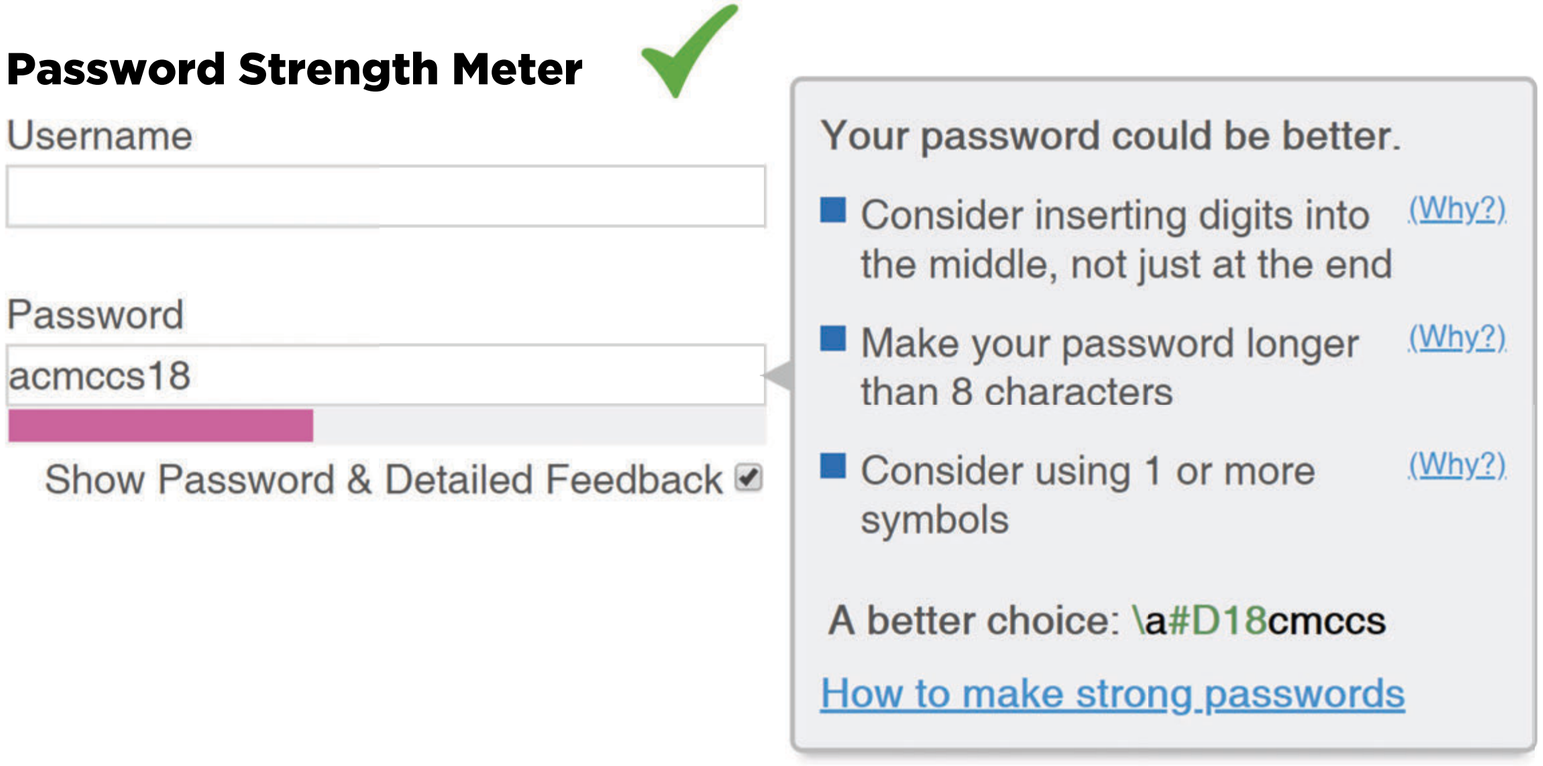
Memory-Hard Hash Function ✓

Email	Argon2i Hash of Password
…	…
jim@mail.com	$argon2i$v=19$m=4096,…
…	…

Rate-Limiting Guessing ✓



Password Strength Meter ✓



AcmeCo

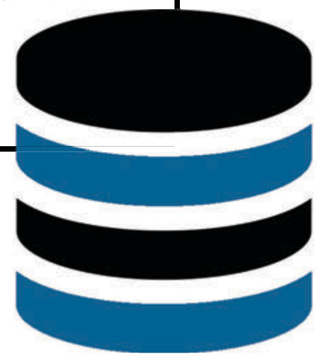
Email
...
jim@mail.com
...

LinkedIn

Email
jane@aol.com
jessey@gmx.net
jenny@gmail.com
jim@mail.com
john@hotmail.com
...

LinkedIn

Email	SHA-1 Hash of Password
jane@aol.com	7c4a8d09ca3762af61e595209
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	7c222fb2927d828af22f59213
jim@mail.com	ba93664a90285b9ff18a7a081
john@hotmail.com	b1b3773a05c0ed0176787a4f1
...	...

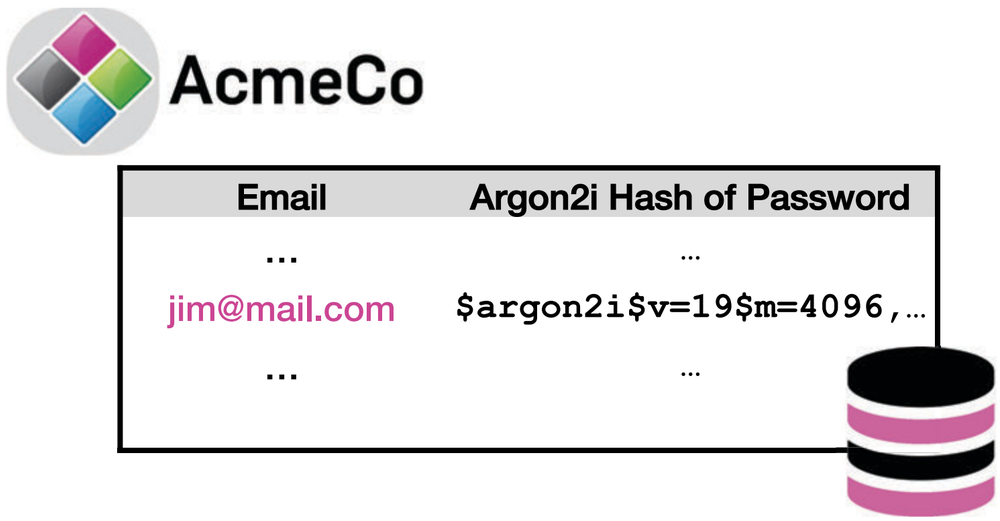


crack all the things!

```
Bash
$> hashcat –m 100 –a0 $TARGET $DICT
123456
Password
ROcky!17
Football!17
CanadaRocks!
```

Email	Cracked SHA-1 Hashes
jane@aol.com	123456
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	Canada4ever
jim@mail.com	ROcky!17
john@hotmail.com	HikingGuy89
…	…

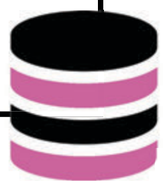
dead on arrival



dead on arrival

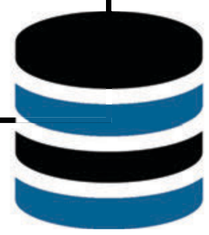
AcmeCo

Email	Argon2i Hash of Password
…	…
jim@mail.com	`$argon2i$v=19$m=4096,…`
…	…



LinkedIn

Email	Cracked SHA-1 Hashes
jane@aol.com	`123456`
jessey@gmx.net	`5baa61e4c9b93f3f0682250b6`
jenny@gmail.com	`Canada4ever`
jim@mail.com	`R0cky!17`
john@hotmail.com	`HikingGuy89`
…	…



dead on arrival

AcmeCo

Email	Cracked
…	…
jim@mail.com	R0cky!17
…	…

LinkedIn

Email	Cracked SHA-1 Hashes
jane@aol.com	123456
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	Canada4ever
jim@mail.com	R0cky!17
john@hotmail.com	HikingGuy89
…	…

1 guess is enough!

LILY HAY NEWMAN SECURITY 10.03.17 07:29 PM

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

Anatomy of a password disaster: Adobe's gian

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

RISK ASSESSMENT —

How LinkedIn's password sloppiness hurts us all

ure dumps.

guardian

all sections

Adobe,

';--have i been pwned?

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

314	5,555,329,164	80,540	87,820,647
pwned websites	pwned accounts	pastes	paste accounts

Facebook

Facebook sa[illegible] had personal data stolen in recent breach

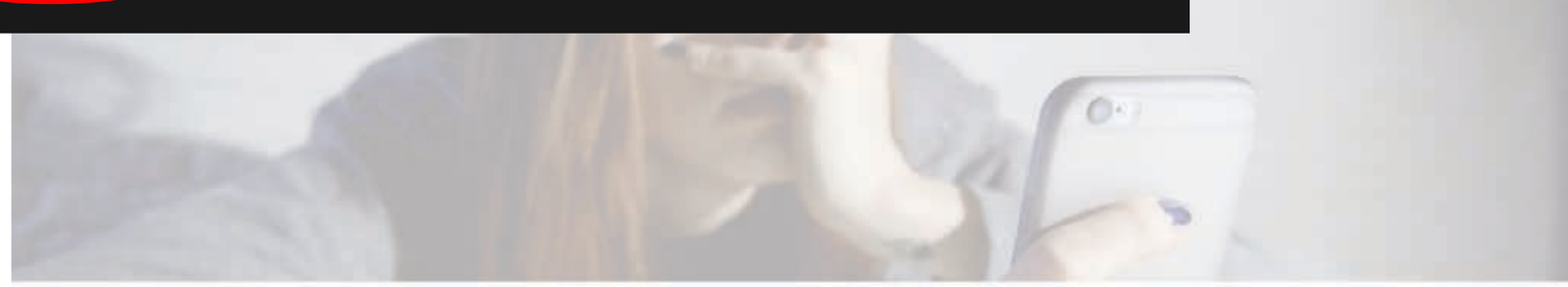
Hackers were able to access name, birthdate and other data in nearly half of the 30 million accounts that were affected

facebook

Email or Phone Password

Sign Up

Connect with friends and the



You Can Now Look Up Your Terrible 2006 MySpace Password

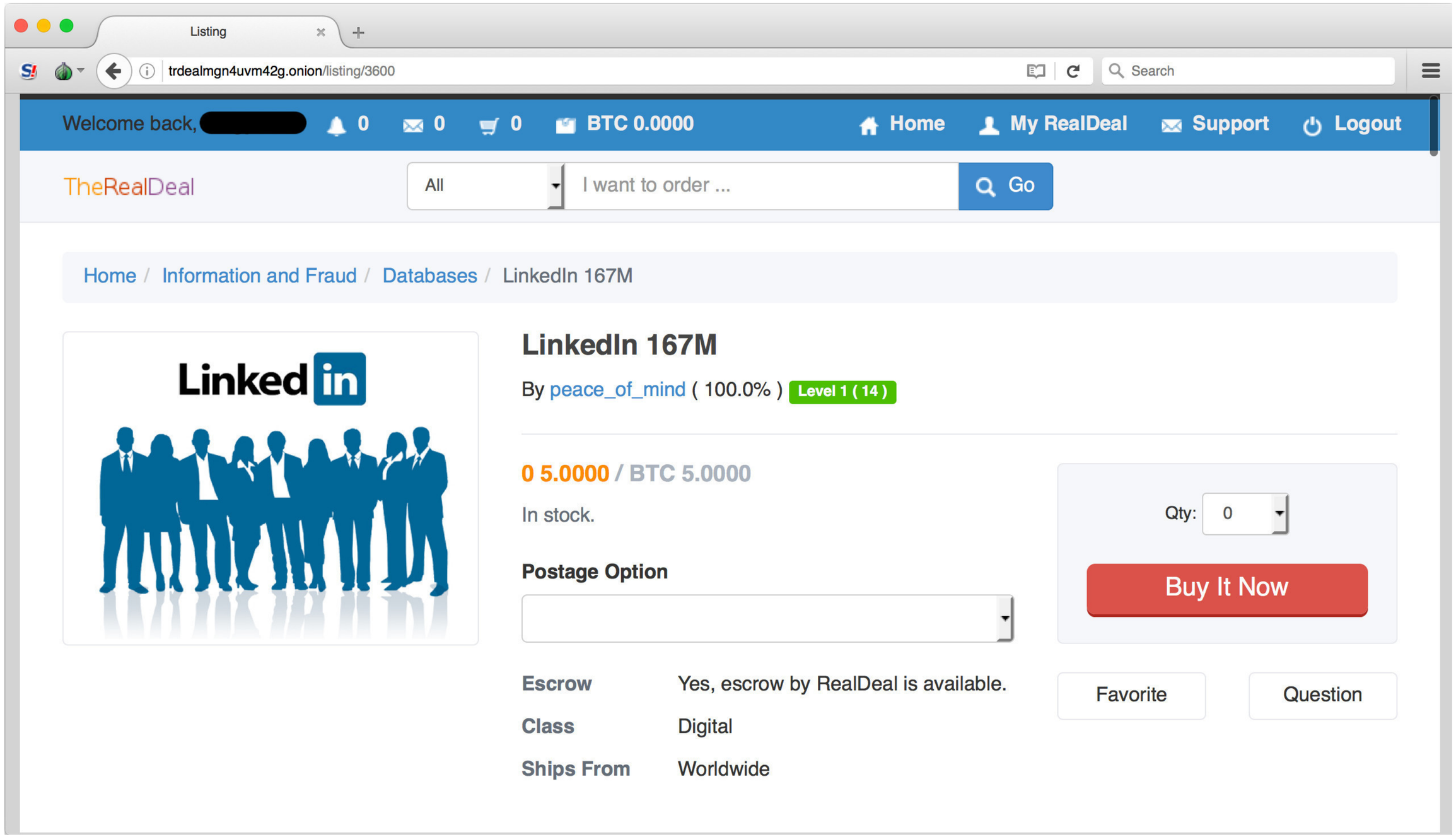
June 29, 2016 // 11:35 AM EST

Written by

LORENZO FRANCESCHI-BICCHIERAI

STAFF WRITER

black market monitoring



black market monitoring

BEST PRODUCTS REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS JOIN / SIGN IN

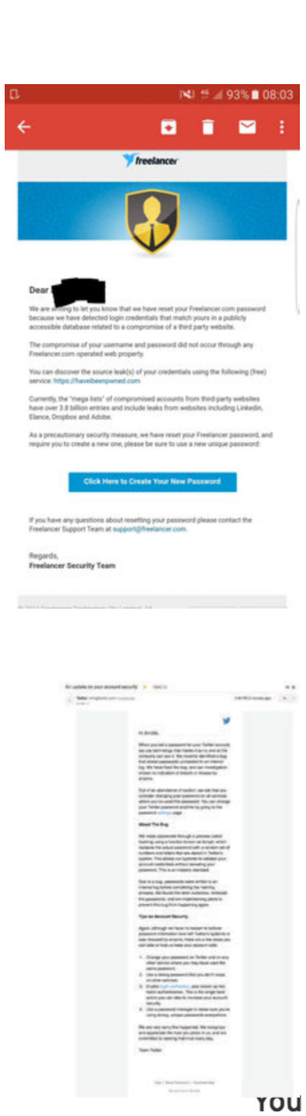
SECURITY

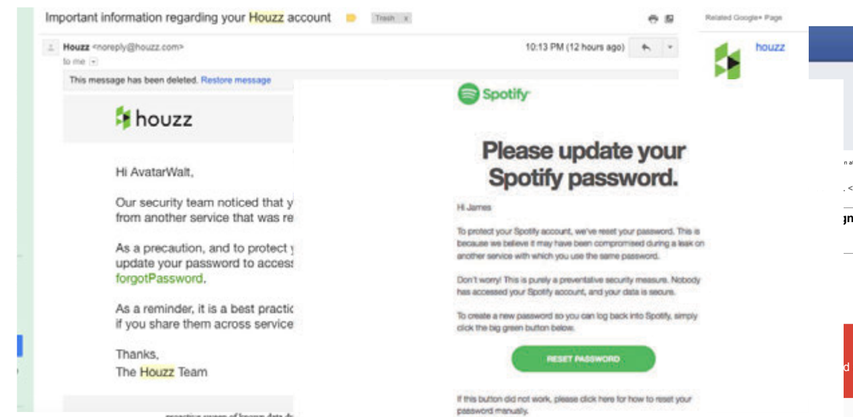
Facebook buys black market passwords to keep your account safe

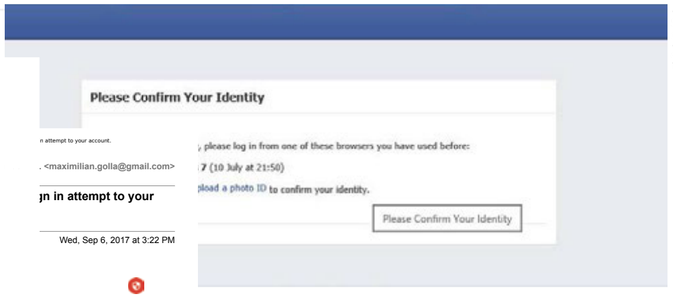
The company's security chief says account safety is about more than just building secure software.

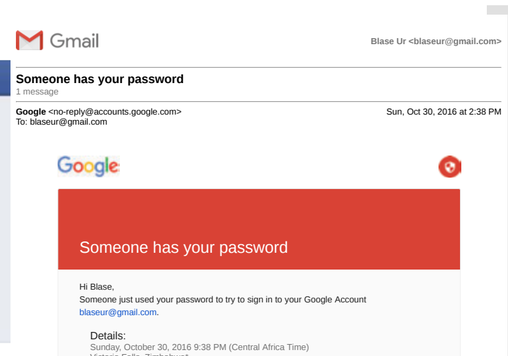
BY KATIE COLLINS | NOVEMBER 9, 2016 12:56 PM PST

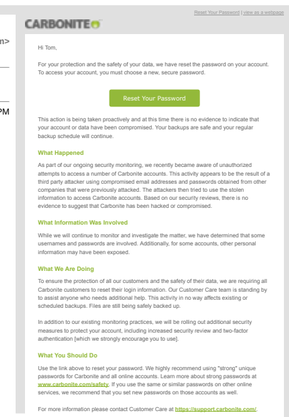
what's the state-of-the-art?

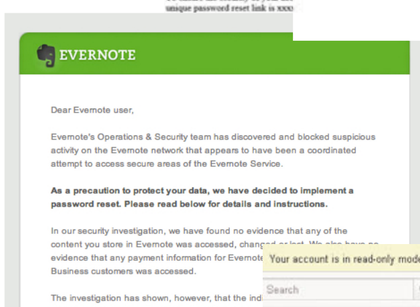


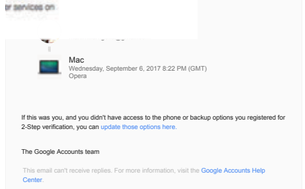


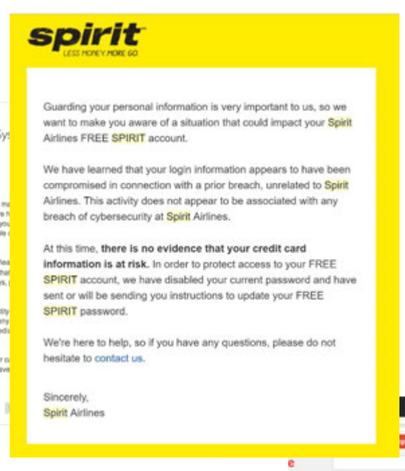


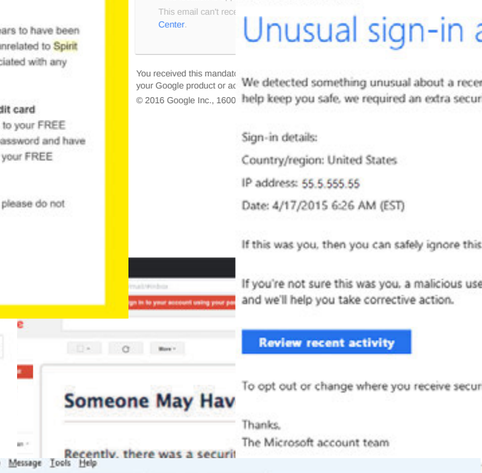


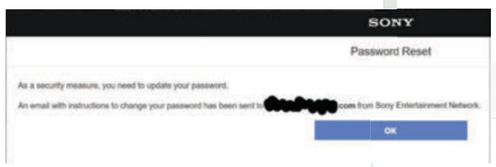


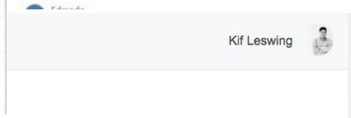


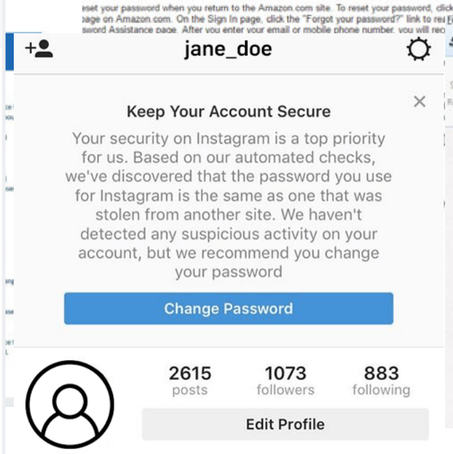


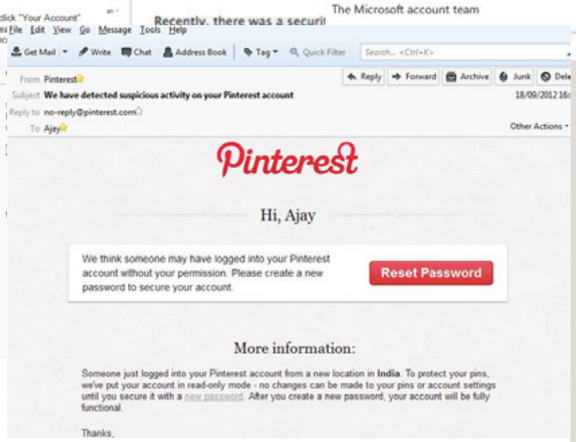


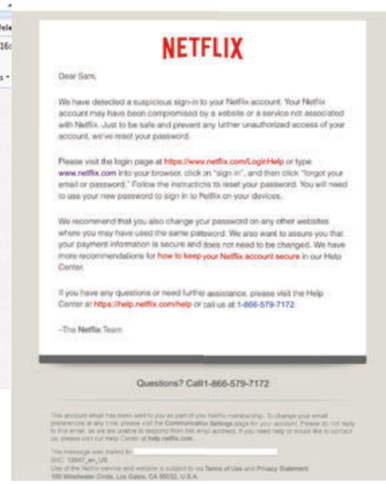


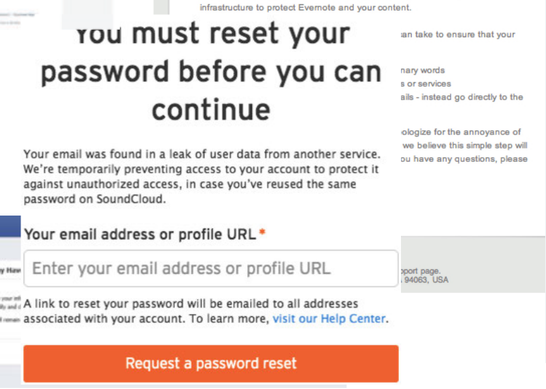


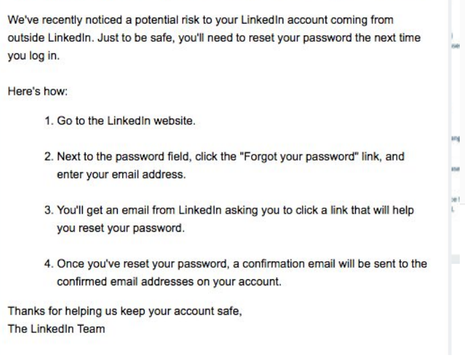










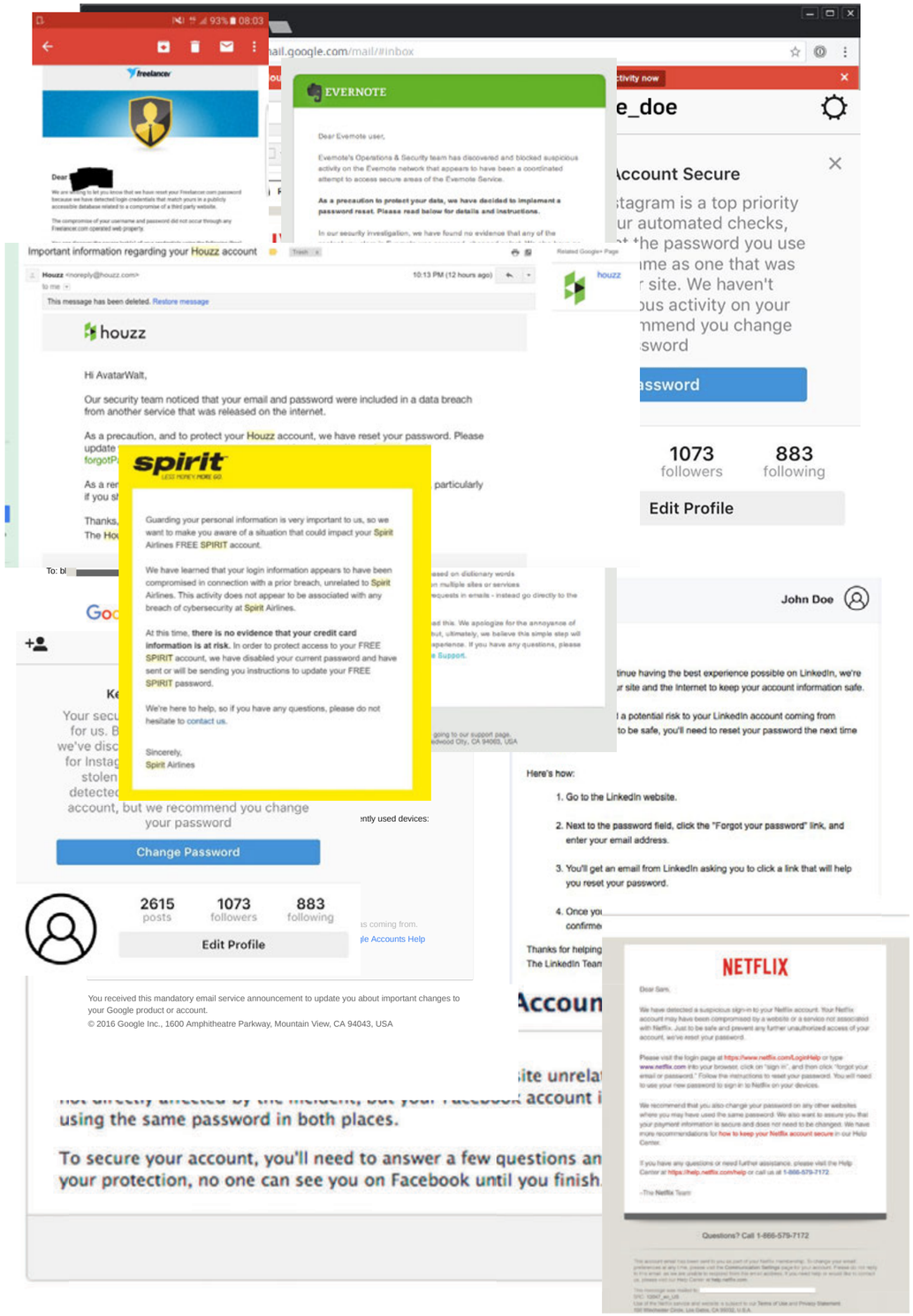


Keep your account secure

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

24 notifications



6 representative notifications

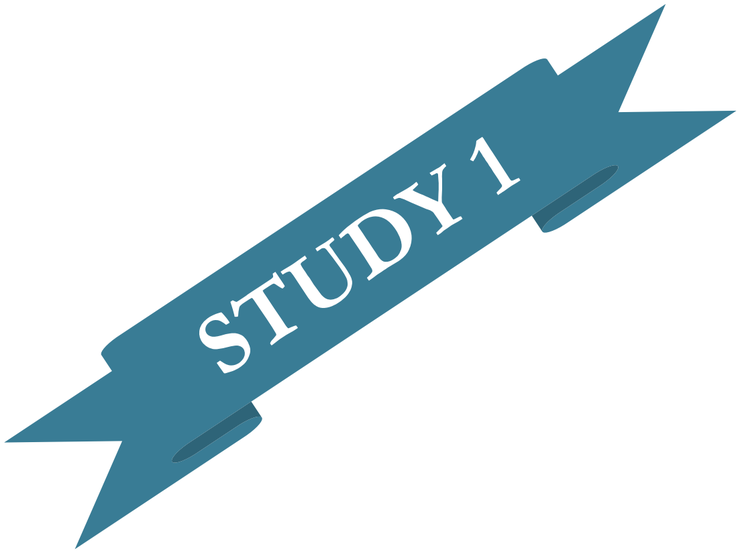
methodology

STUDY 1

previously sent password-reuse notifications

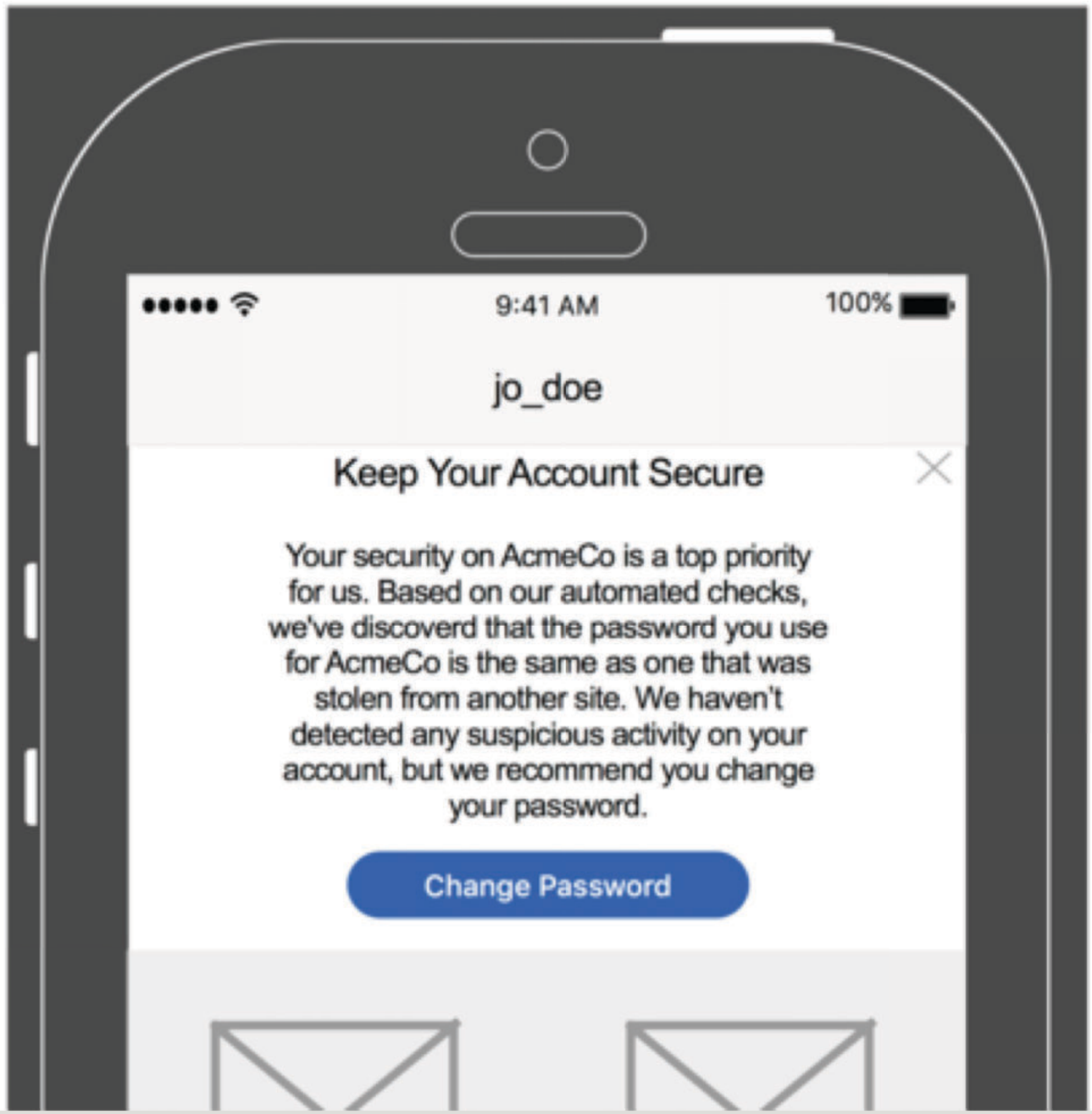
STUDY 2

individual components of password-reuse notifications



Imagine you have an important account with AcmeCo...

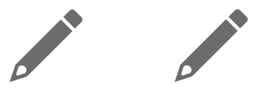
AcmeCo notifications



1

questions asked

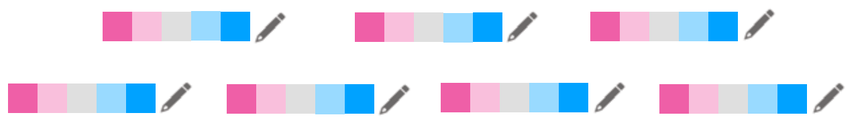
notification understanding



feelings

actions

perceptions



demographics

1

survey setup

180 respondents

- Amazon MTurk
- 15 mins
- Compensated $2.50

6 conditions

1

notifications were concerning and a priority

surprised

safe

annoyance

anxious

nervous

worried

concerned

afraid

angry

confusion

83%

very high or high priority

1

Why did you receive this notification?

60% hacked account

21% data breach

1

don’t mention password reuse

allude to password reuse

0 - 4% respondents

48 - 56% respondents

listed password reuse as a cause


Keep Your Account Secure
Your security on Instagram is a top priority for us. Based on our automated checks, we've discovered that the password you use for Instagram is the same as one that was stolen from another site. We haven't detected any suspicious activity on your account, but we recommend you change your password
Change Password

Keep Your Account Secure

Your security on Instagram is a top priority for us. Based on our automated checks, we've discovered that the password you use for Instagram is the same as one that was stolen from another site. We haven't detected any suspicious activity on your account, but we recommend you change your password

Change Password

1

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

STUDY 1 CONCLUSIONS

Current password-reuse notifications

✓ elicit concern

✗ explain the situation

five notification goals

timely

sufficient background

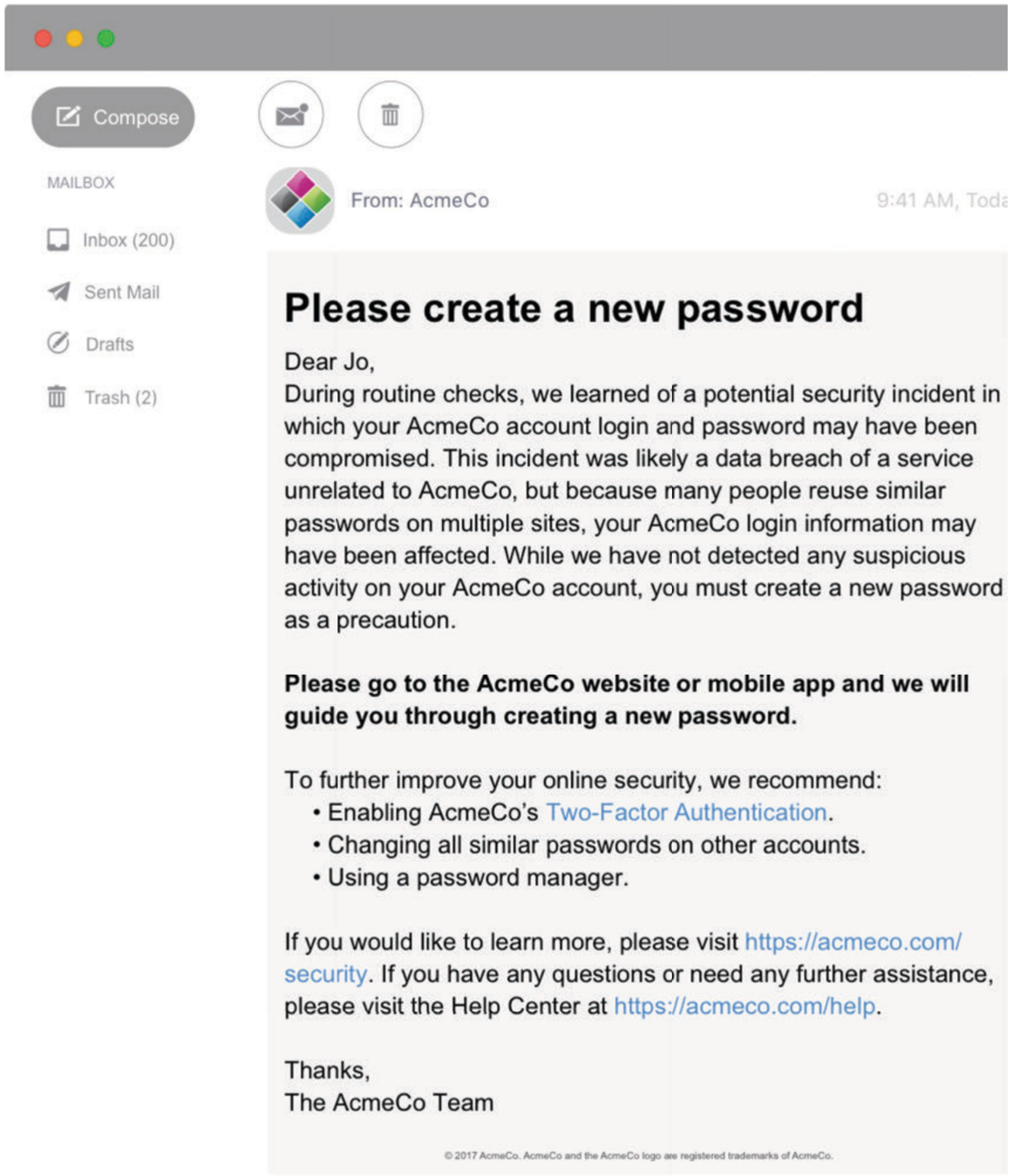
secure actions

legitimate

trust

STUDY 2

our model notification



2

survey setup

588 respondents

- Amazon MTurk
- 15 mins
- Compensated $2.50

15 conditions

DELIVERY MEDIUM

INCIDENT DESCRIPTION

ACCOUNT ACTIVITY

PASSWORD CHANGE

EXTRA SUGGESTIONS

OTHER ACCOUNTS

2

What would you do about your AcmeCo password?

Keep it the same	**6%**
Change it	**90%**
Don’t know	**3%**

2

What would your new password be?

Completely new	**2%**
PW manager/browser	**11%**
Reused password	**13%**
Modified password	**68%**
Other	**6%**

2

“I know my password is already strong and unlikely to be hacked.” (R338)

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

2

“Until I see evidence of hacking, I prefer to keep my own sanity.” (R300)

STUDY 2 CONCLUSIONS

After seeing a password-reuse notification, users

would change passwords

... but ineffectively

have incomplete threat models

conclusion

1. formative, systematic studies of password-reuse notifications

conclusion

1. formative, systematic study of password-reuse notifications

2. developed best practices

best practices

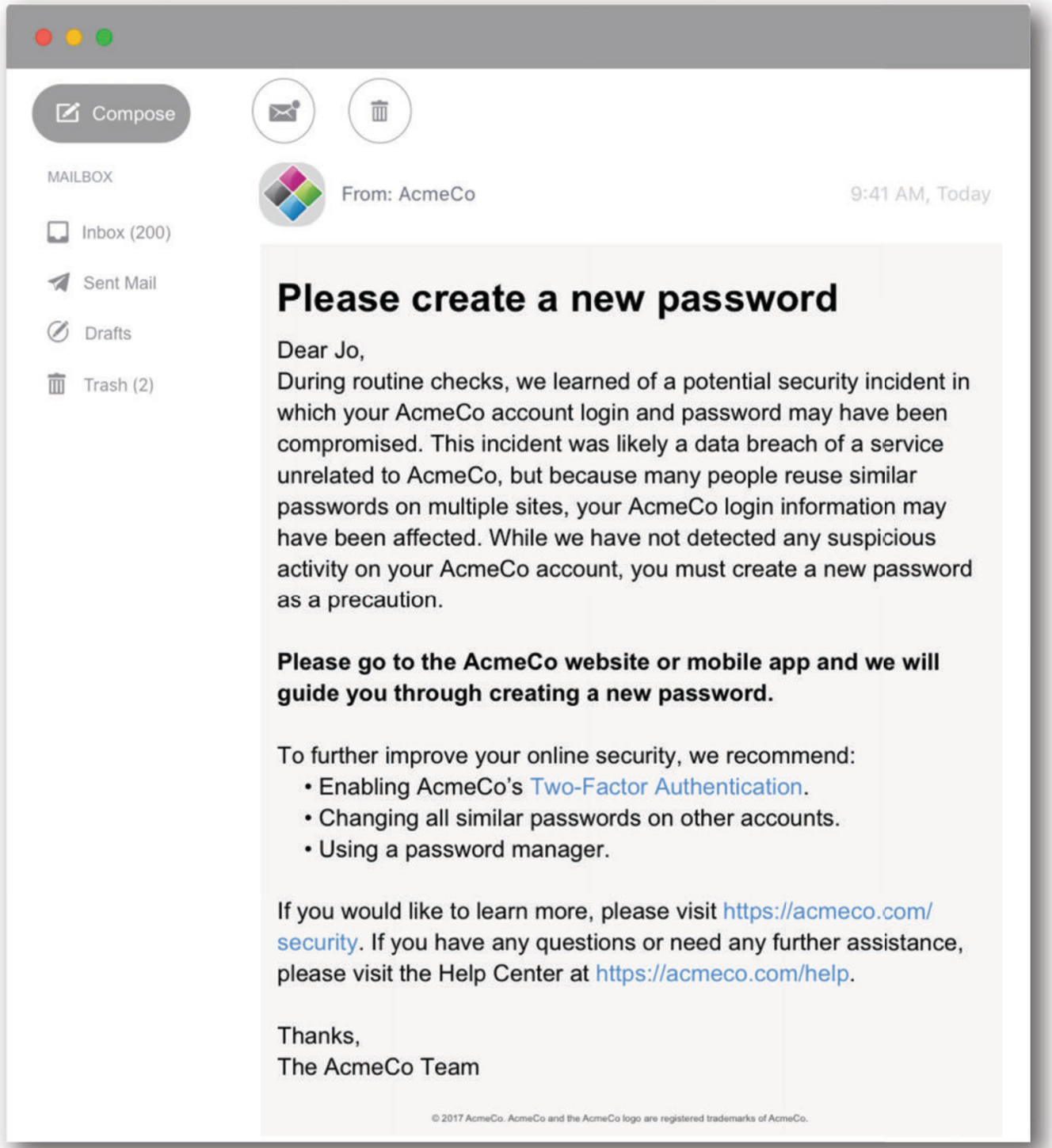
send via email + more immediate channel

name password reuse as root cause

force password reset

encourage 2FA and password managers

suggest unique passwords for other accounts

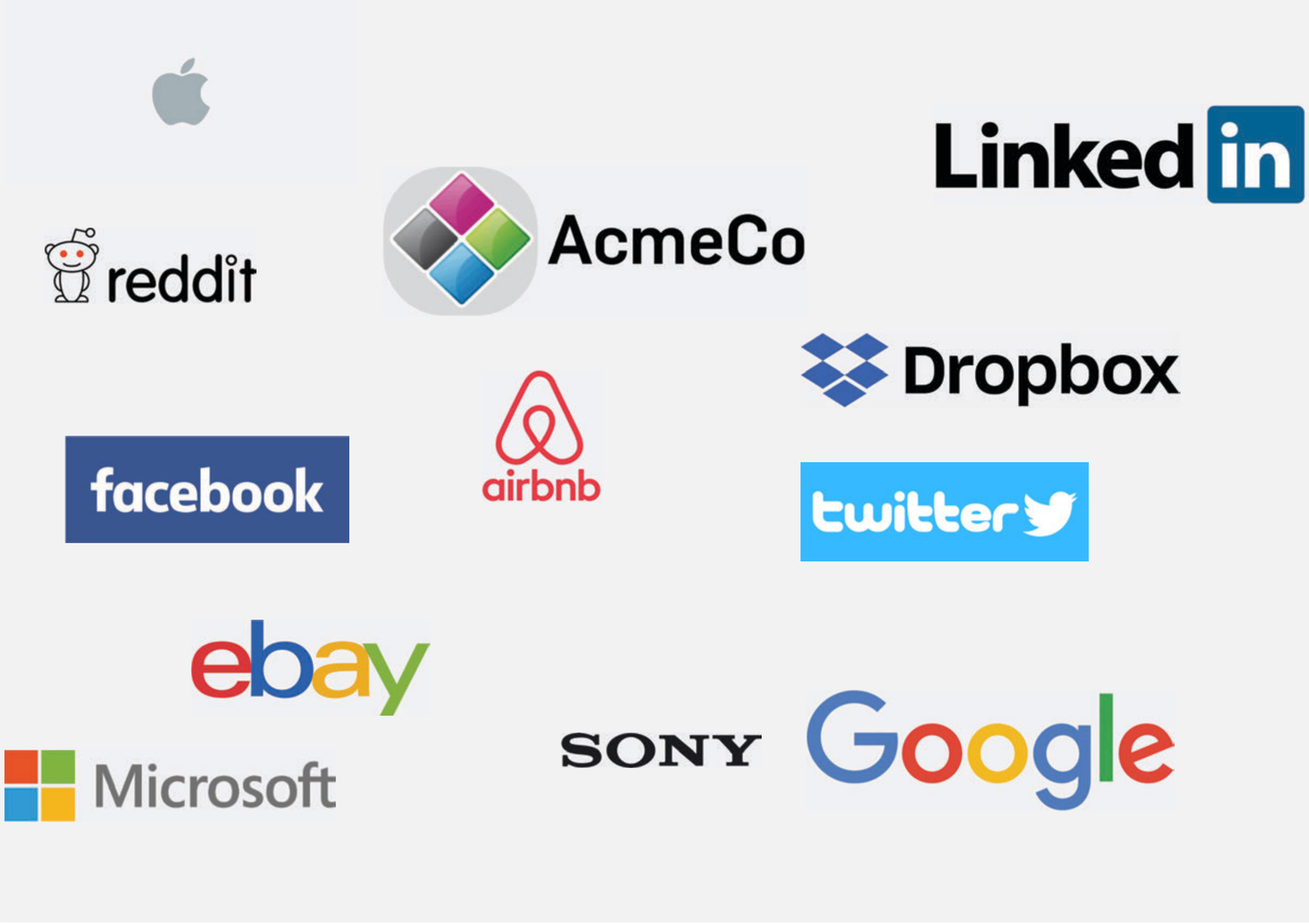

Compose
MAILBOX
Inbox (200)
Sent Mail
Drafts
Trash (2)
From: AcmeCo
9:41 AM, Today
Please create a new password
Dear Jo,
During routine checks, we learned of a potential security incident in which your AcmeCo account login and password may have been compromised. This incident was likely a data breach 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 any 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.

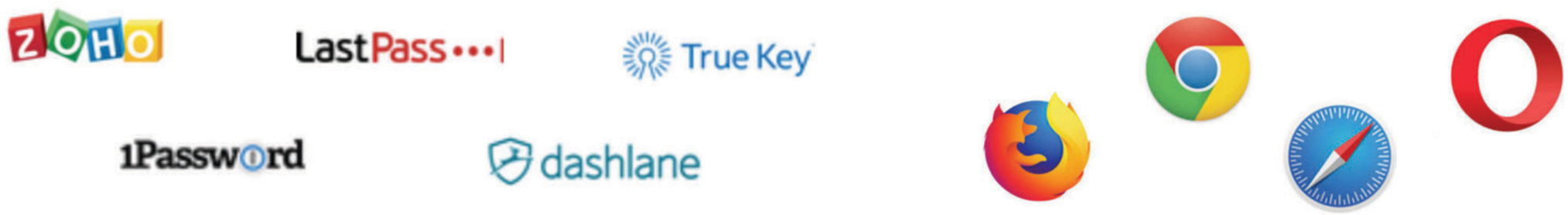
conclusion

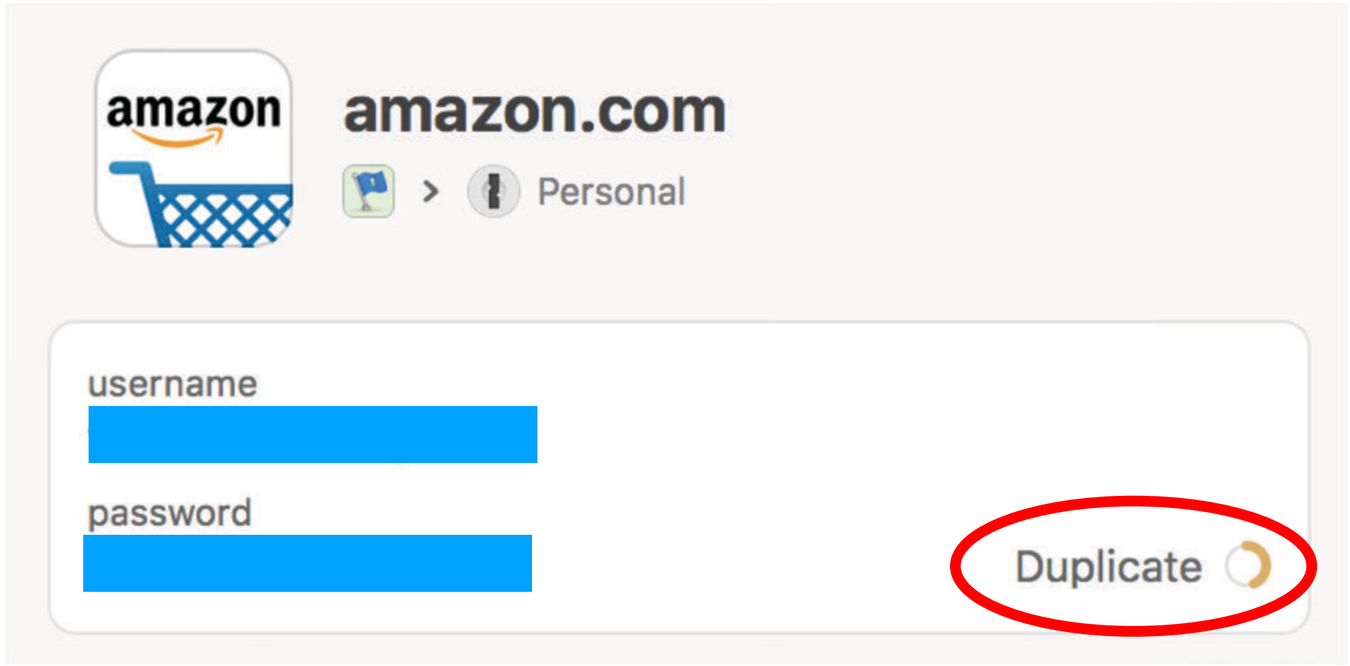
1. formative, systematic study of password-reuse notifications

2. developed best practices

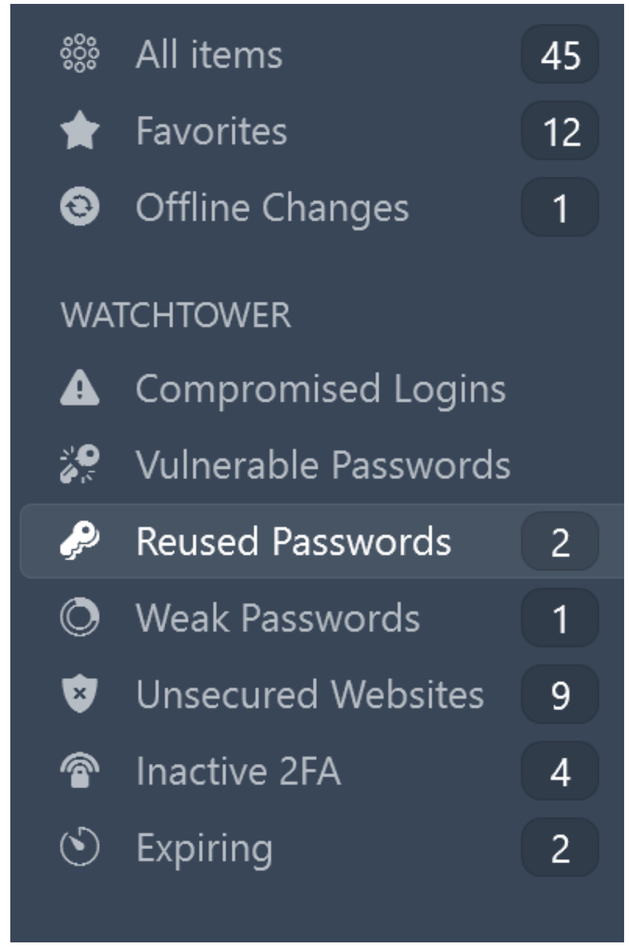
3. future work should study novel notifications

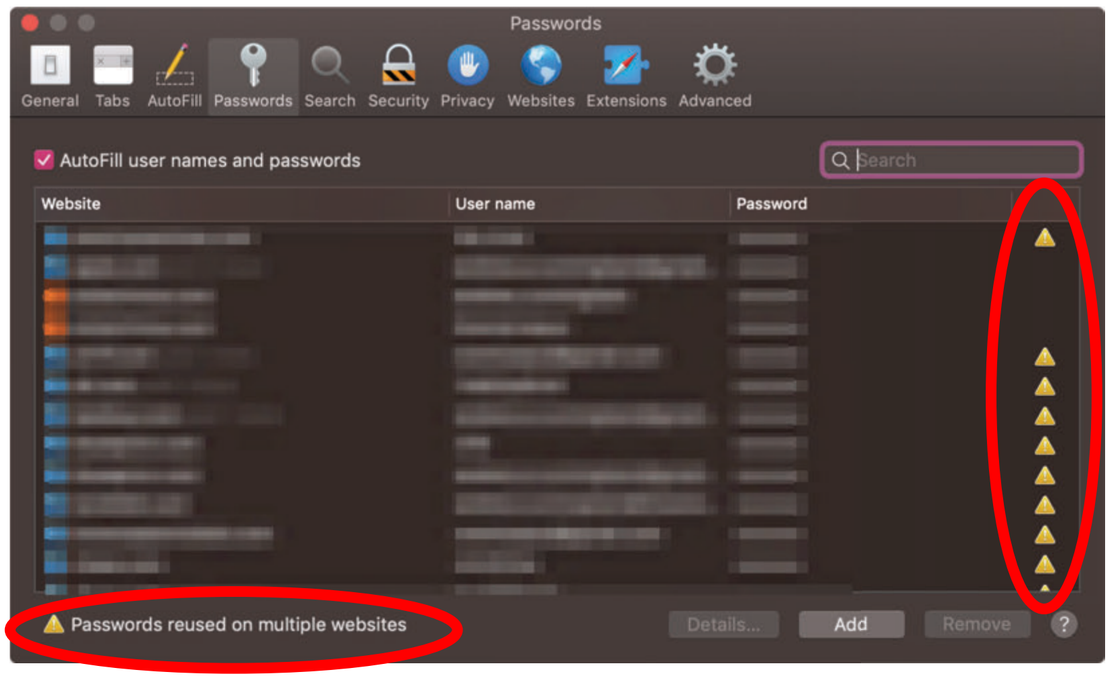

reddit
AcmeCo
LinkedIn
Dropbox
facebook
airbnb
twitter
ebay
Microsoft
SONY
Google


ZOHO
LastPass
True Key
1Password
dashlane



1Password





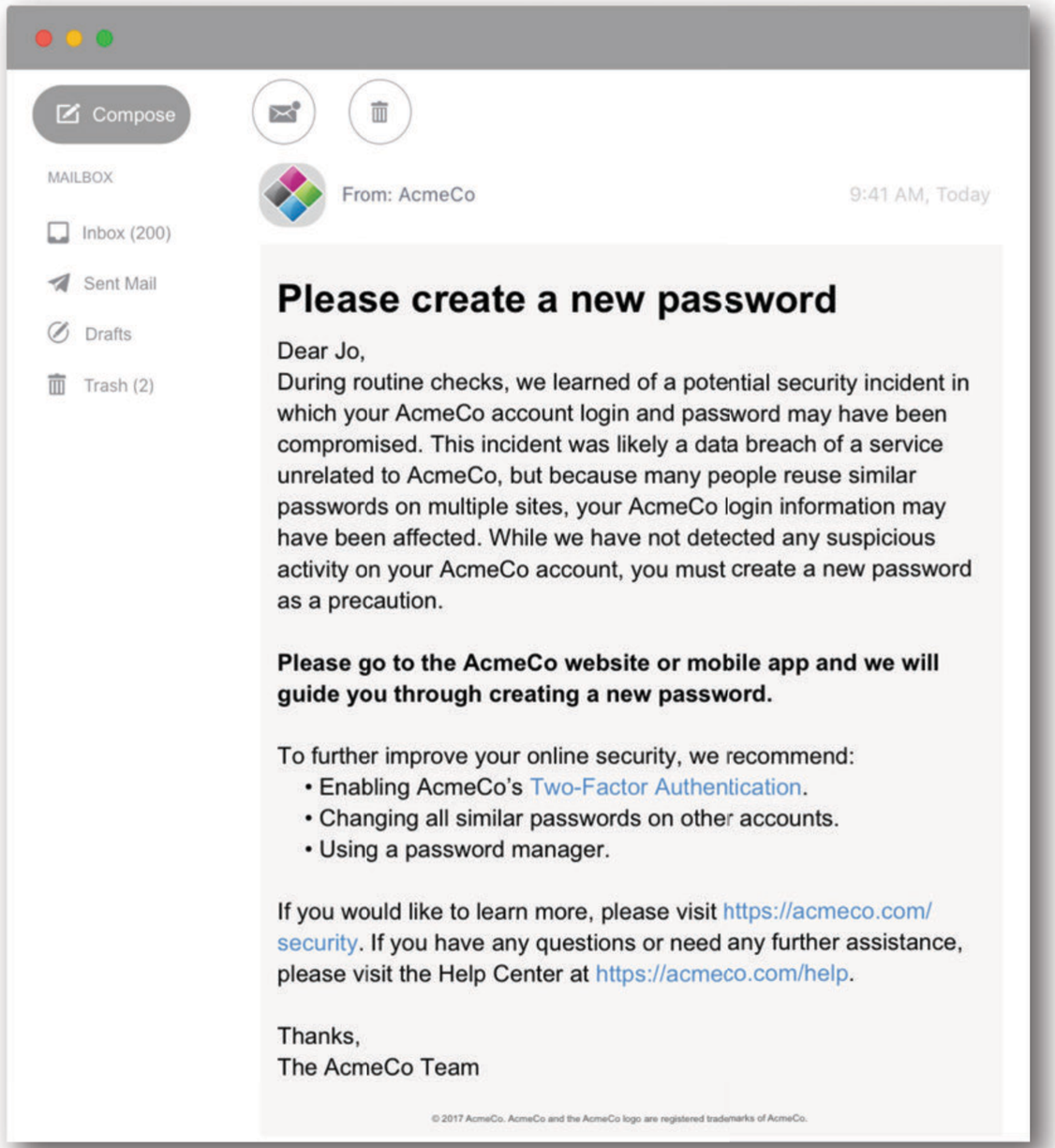
macOS Mojave, Safari 12

conclusion

1. formative, systematic study of password-reuse notifications

2. developed best practices

3. future work should study novel notifications AND find ecosystem-level solutions



Designing Password-Reuse Notifications

Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, Blase Ur

THE UNIVERSITY OF CHICAGO
RUHR UNIVERSITÄT BOCHUM RUB
UNIVERSITY OF MARYLAND
SNIPER GROUP Security, Usability, & Privacy Education & Research