"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

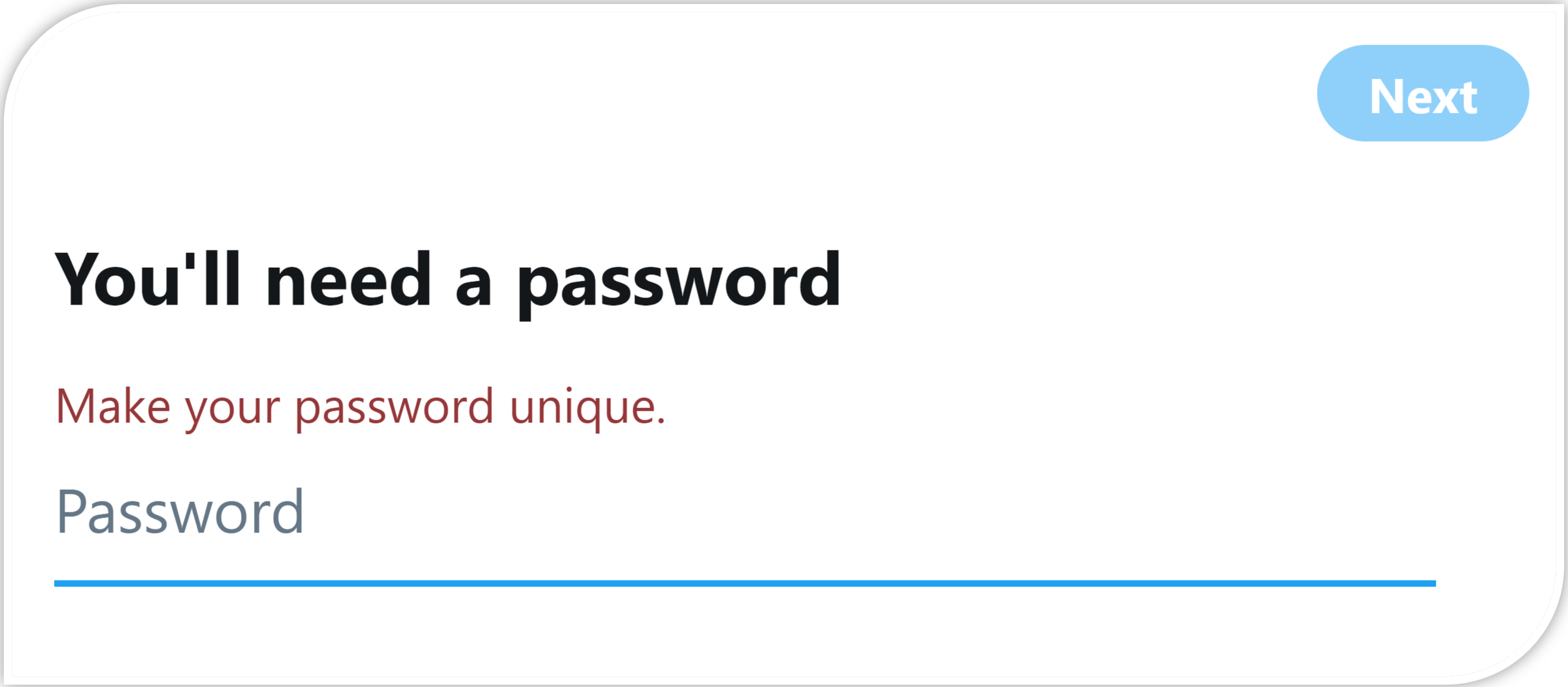
RUHR UNIVERSITÄT BOCHUM RUB

UNIVERSITY OF MARYLAND

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

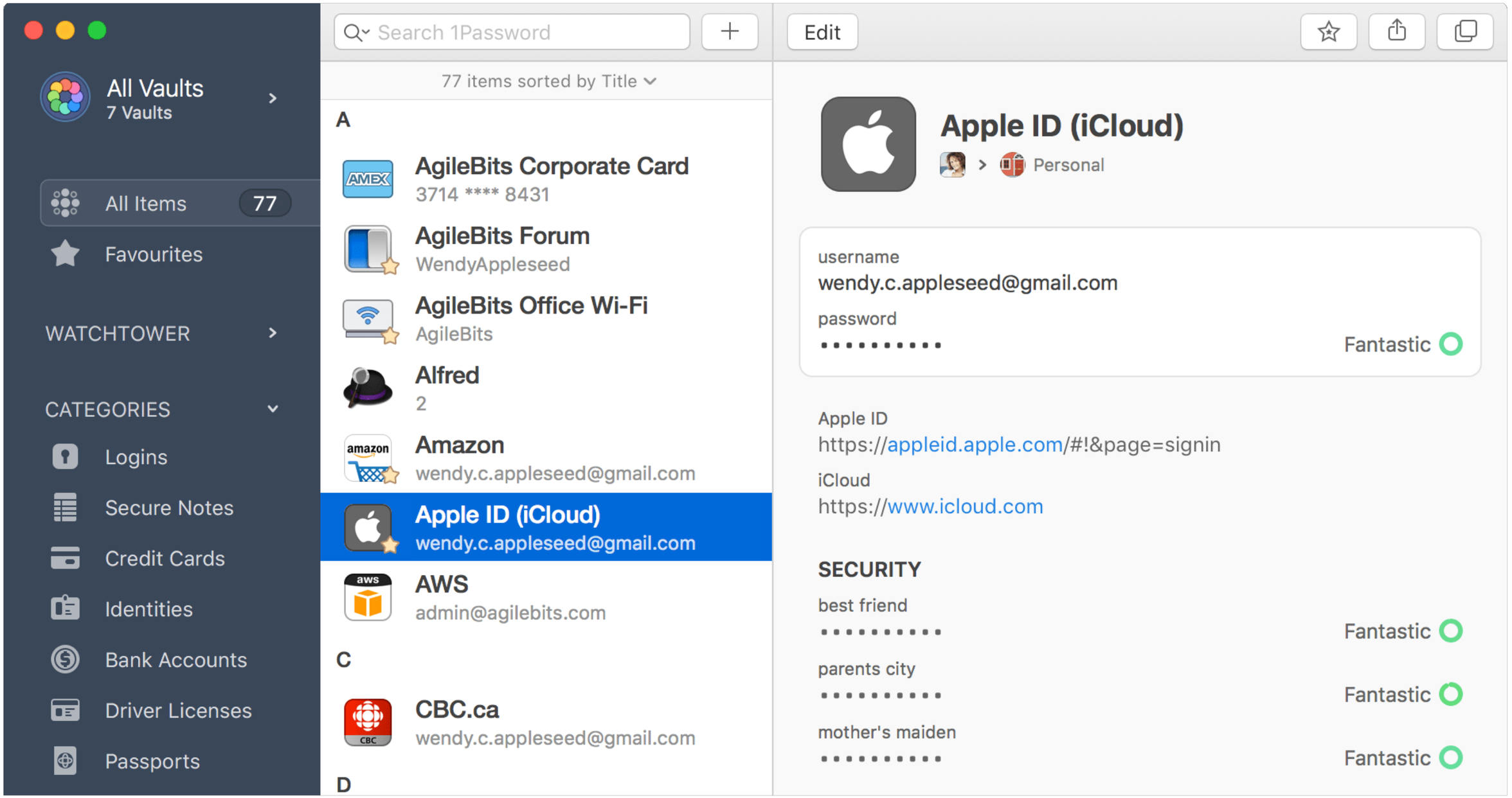
Toronto, Canada | ACM CCS | October 18, 2018

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

R0cky!17

R0ckyBox

R0cky!17

R0cky!17

123456

R0ckyStar

Rocky!16

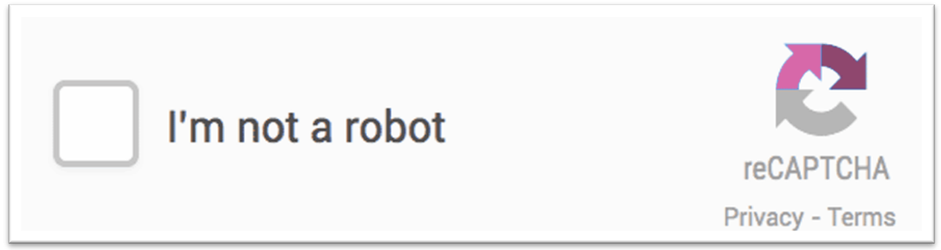
R0cky!17

AcmeCo

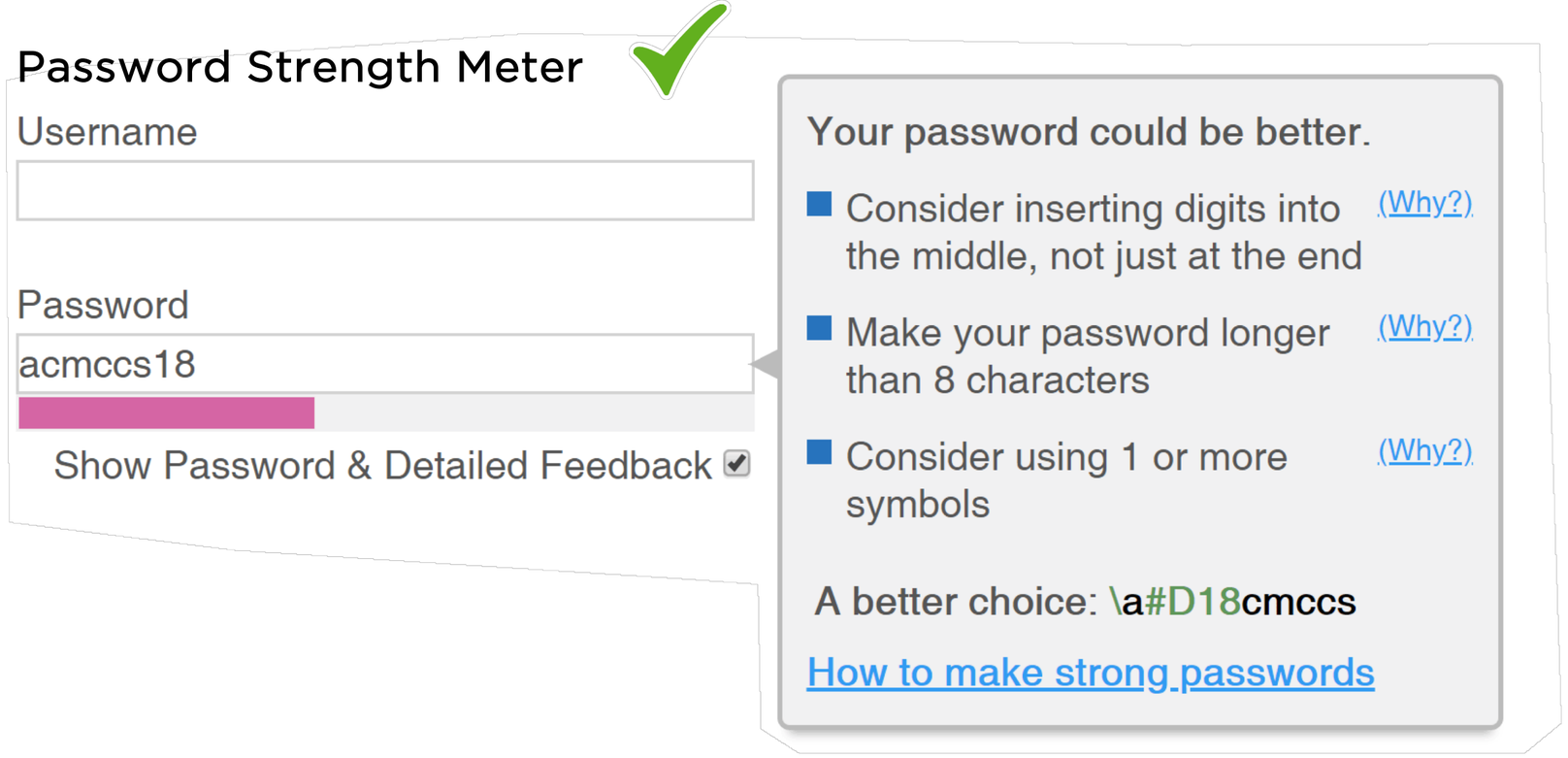
Memory-Hard Hash Function ✓

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

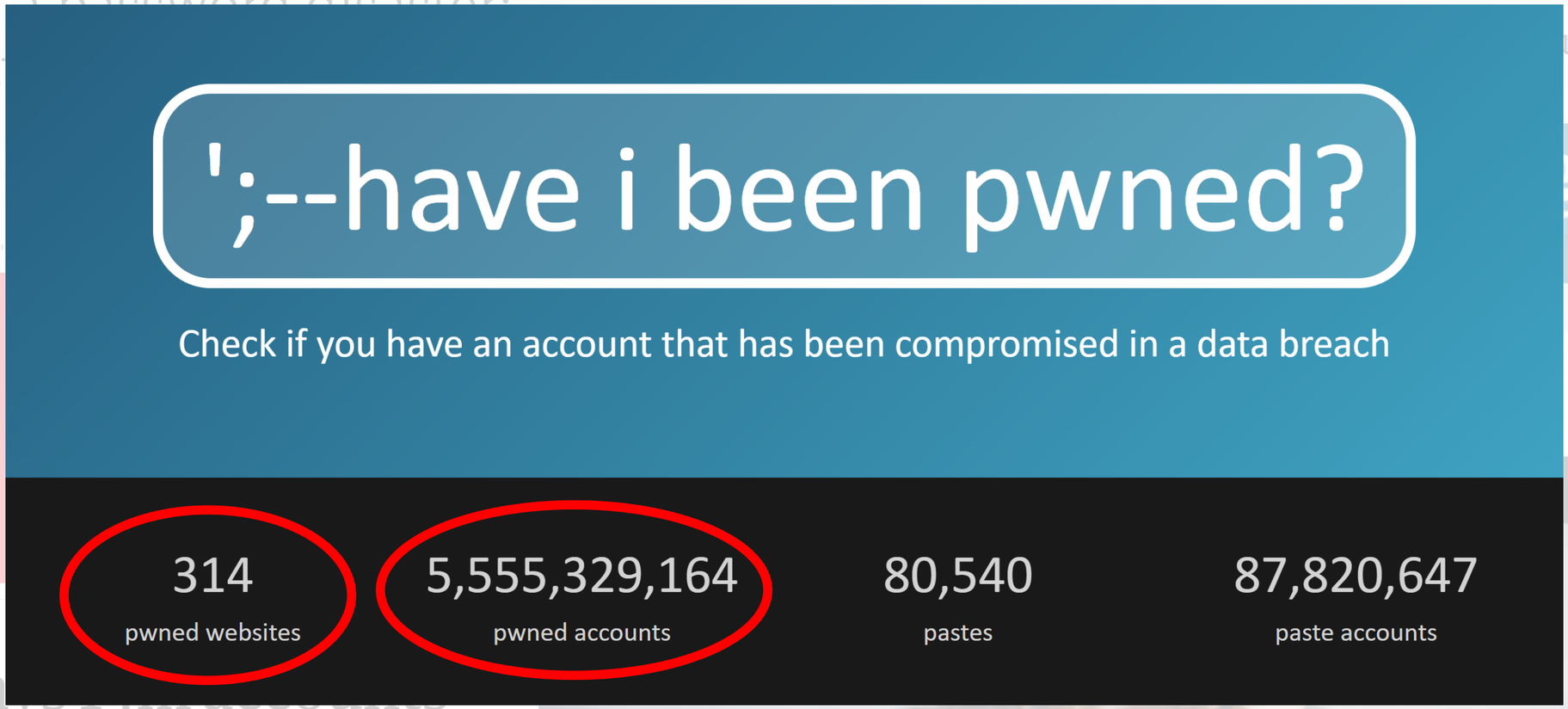
AcmeCo

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

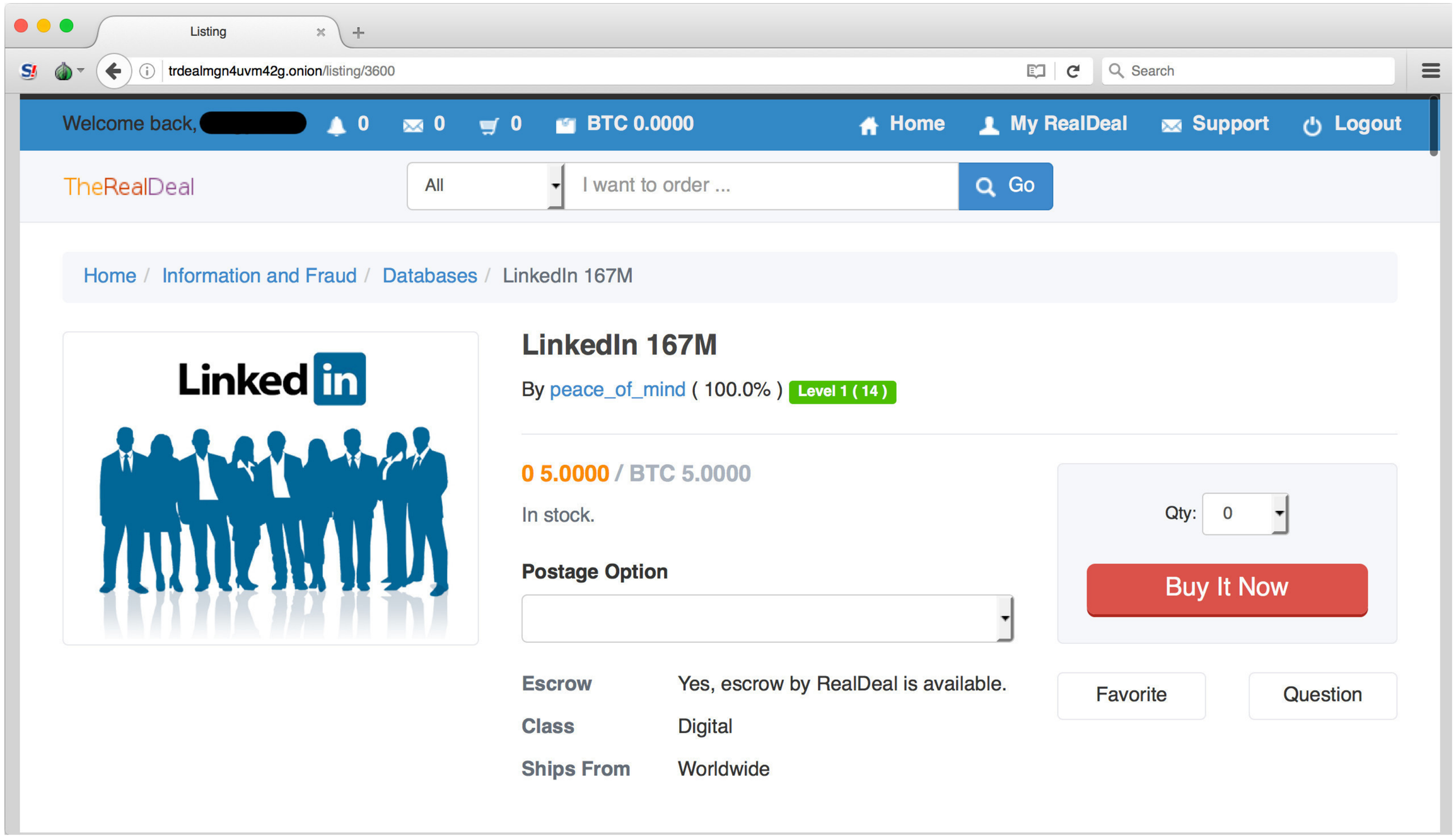
LinkedIn

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
…	…

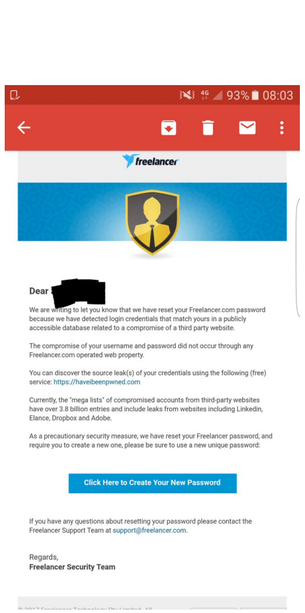
1 guess is enough!

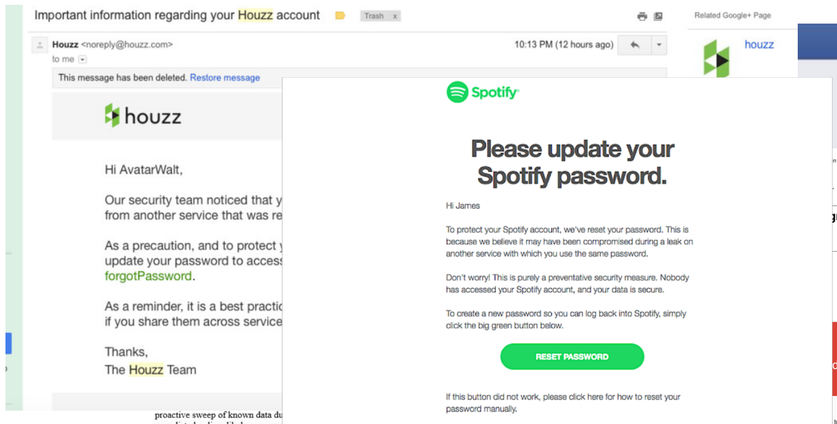

';--have i been pwned?
Check if you have an account that has been compromised in a data breach
314
pwned websites
5,555,329,164
pwned accounts
80,540
pastes
87,820,647
paste accounts

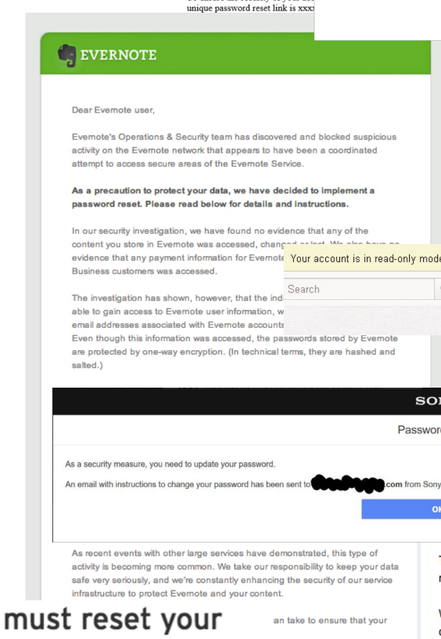
black market monitoring

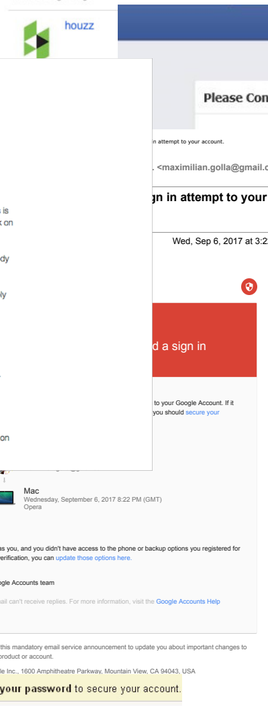


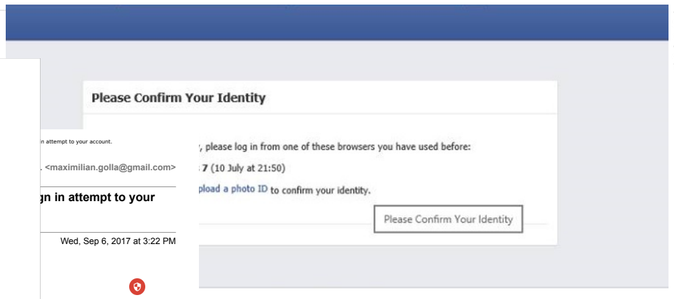
what's the state-of-the-art?

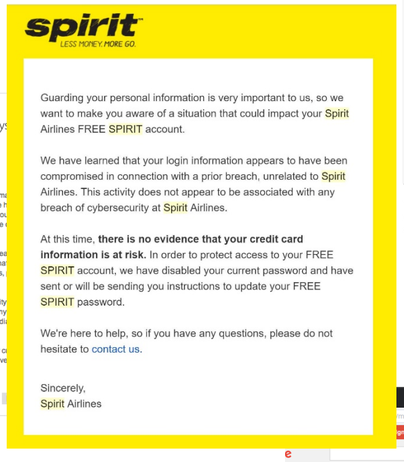


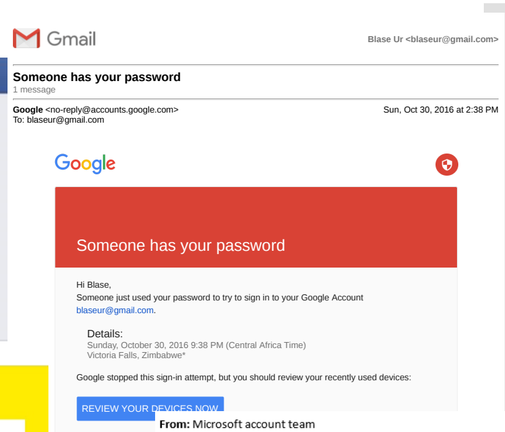


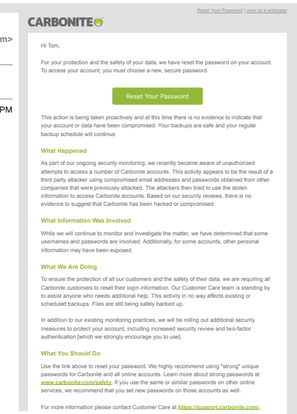


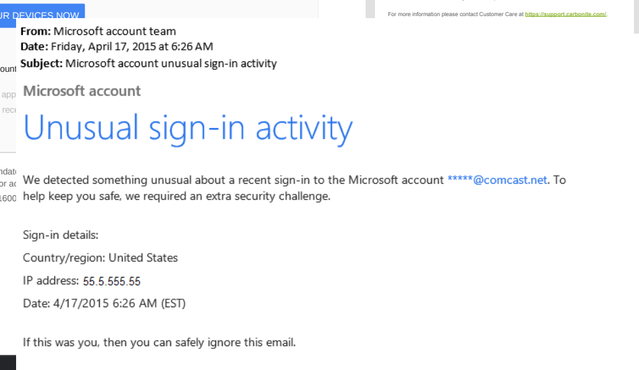


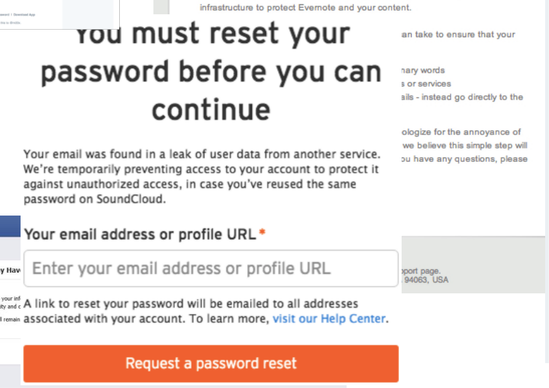


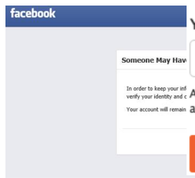


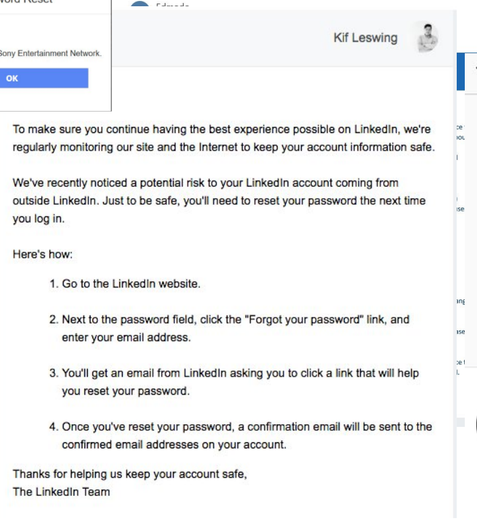


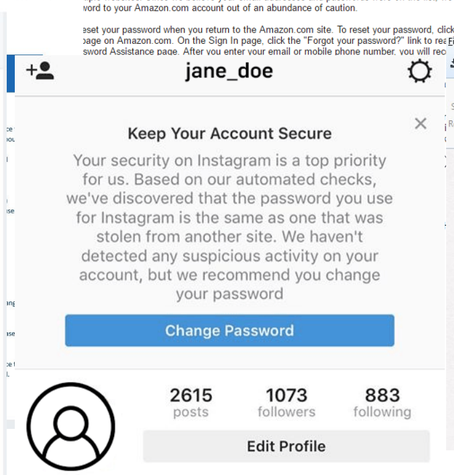


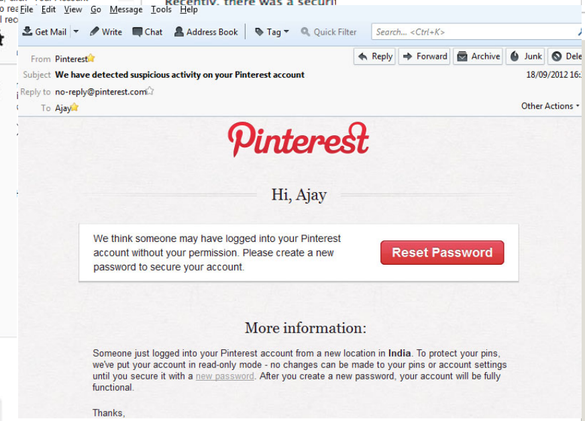


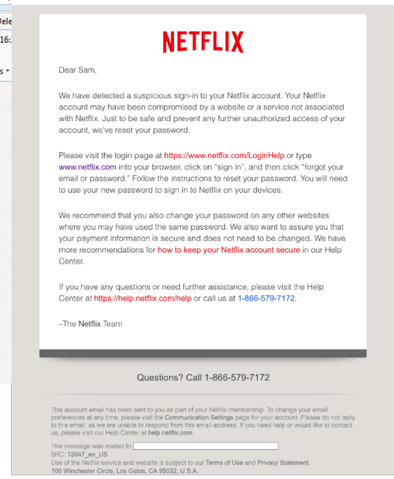












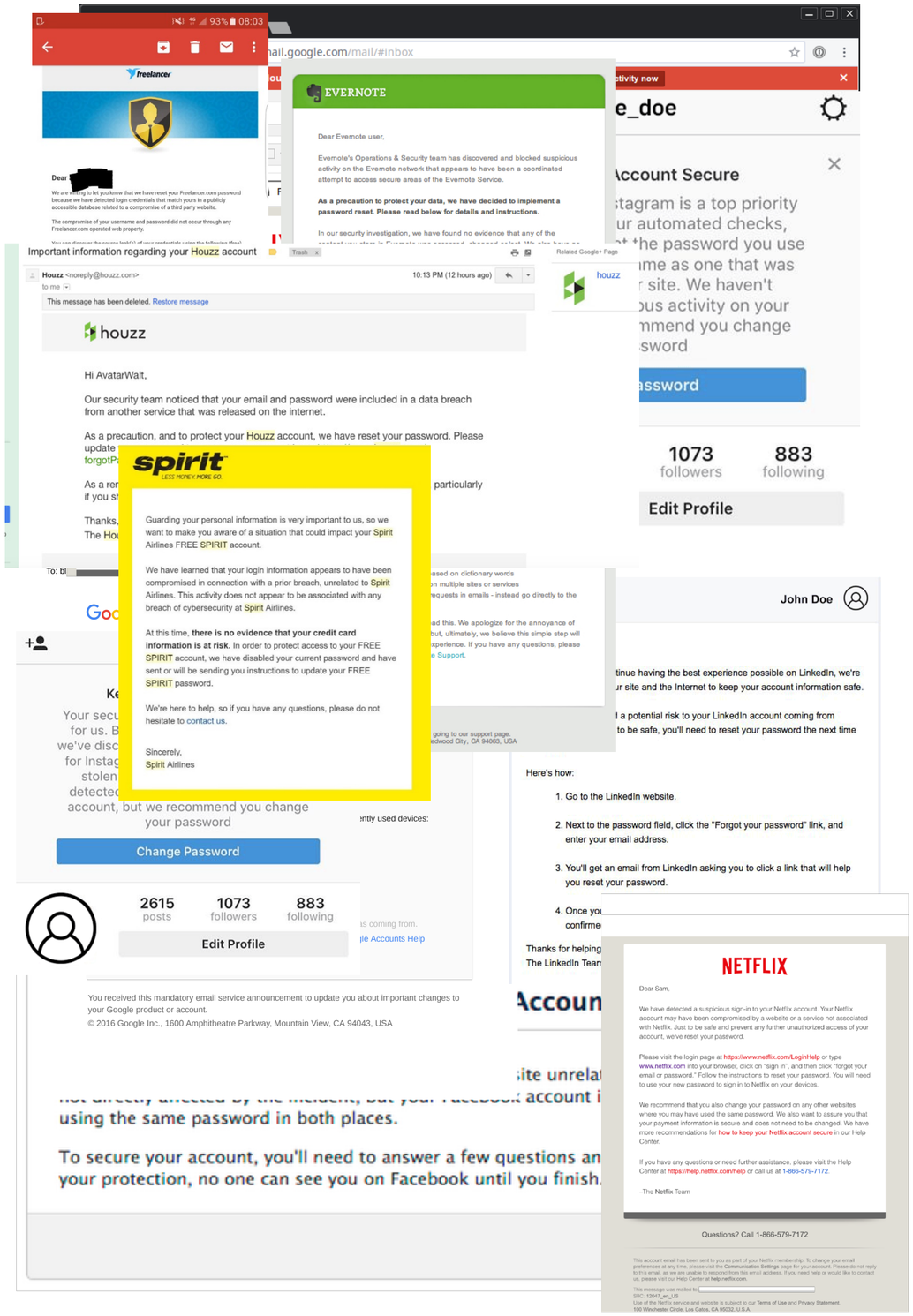
Keep your account secure

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

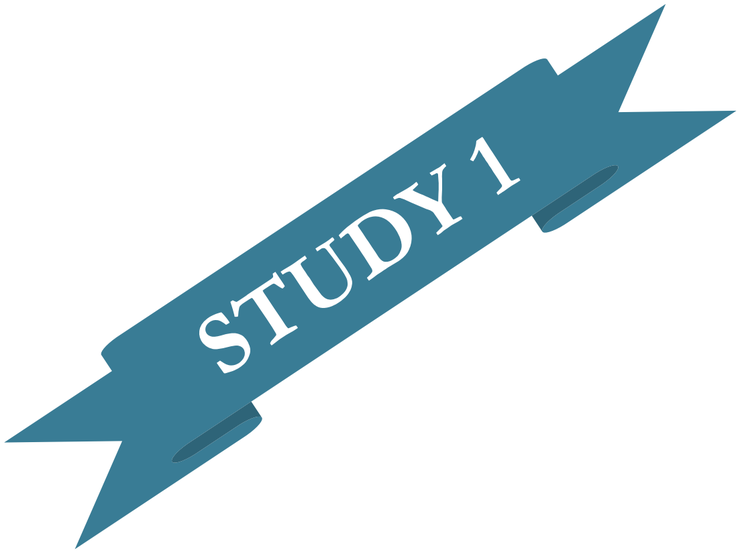
methodology

STUDY 1

previously sent password-reuse notifications

STUDY 2

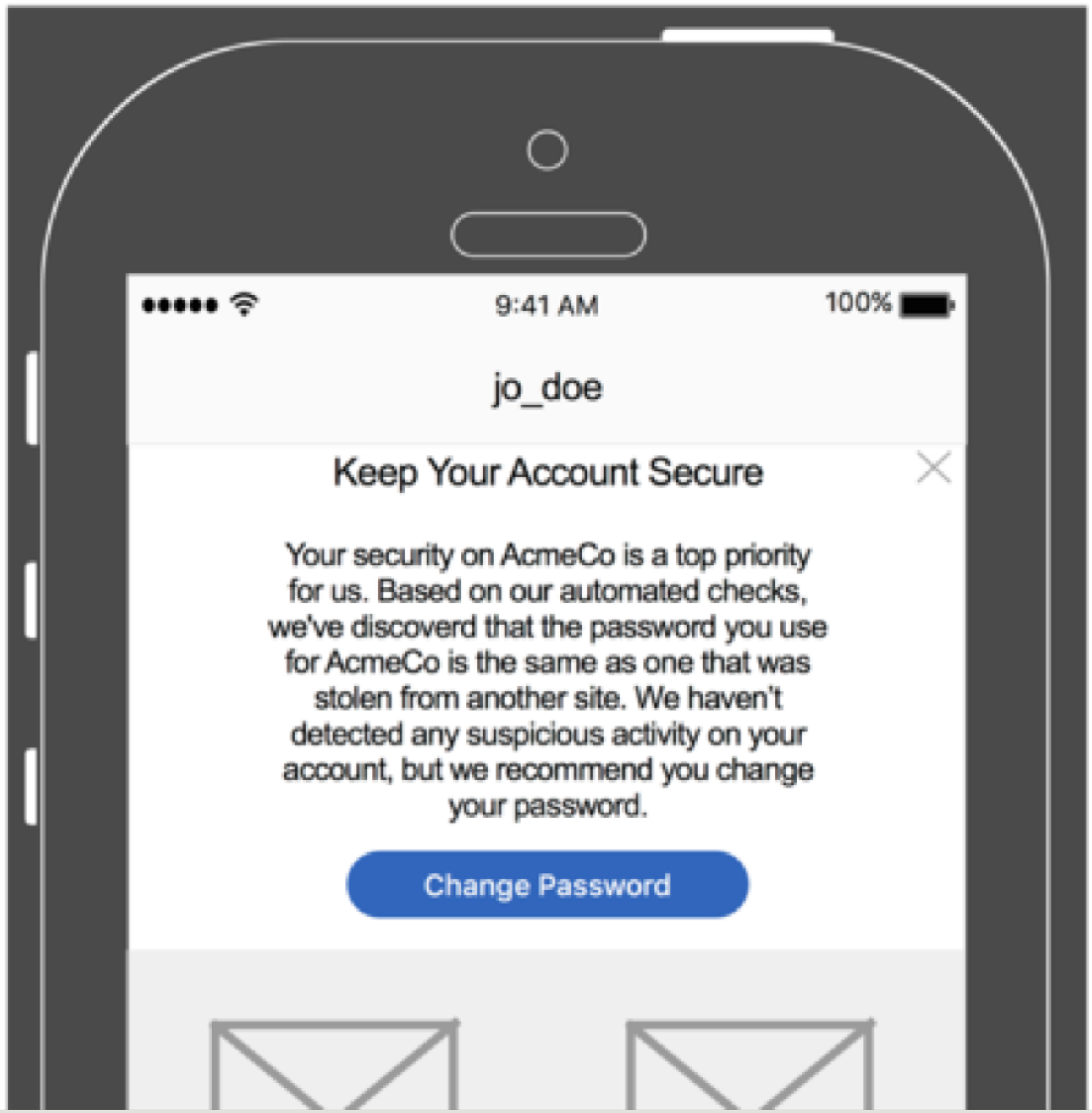
individual components of password-reuse notifications



Imagine you have an important account with AcmeCo…

1

AcmeCo notifications



1

questions asked

notification understanding

feelings

actions

perceptions

demographics

1

survey setup

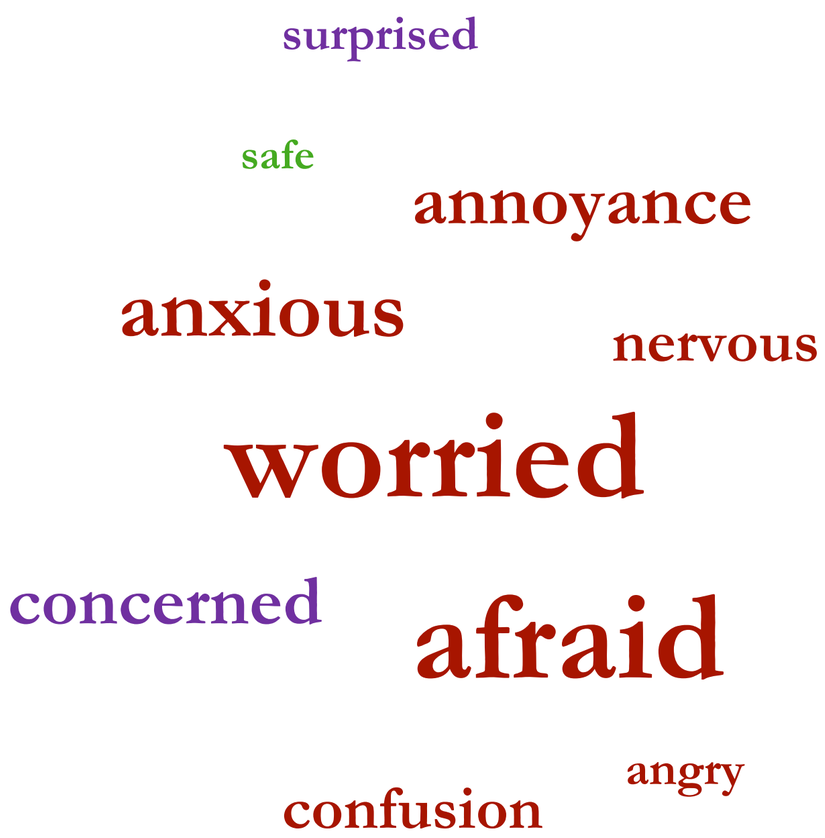
180 respondents

- Amazon MTurk
- 15 mins
- Compensated $2.50

6 conditions

1

notifications were concerning and a priority



83%

very high or high priority

1

Why did you receive this notification?

60% hacked account

21% data breach

1

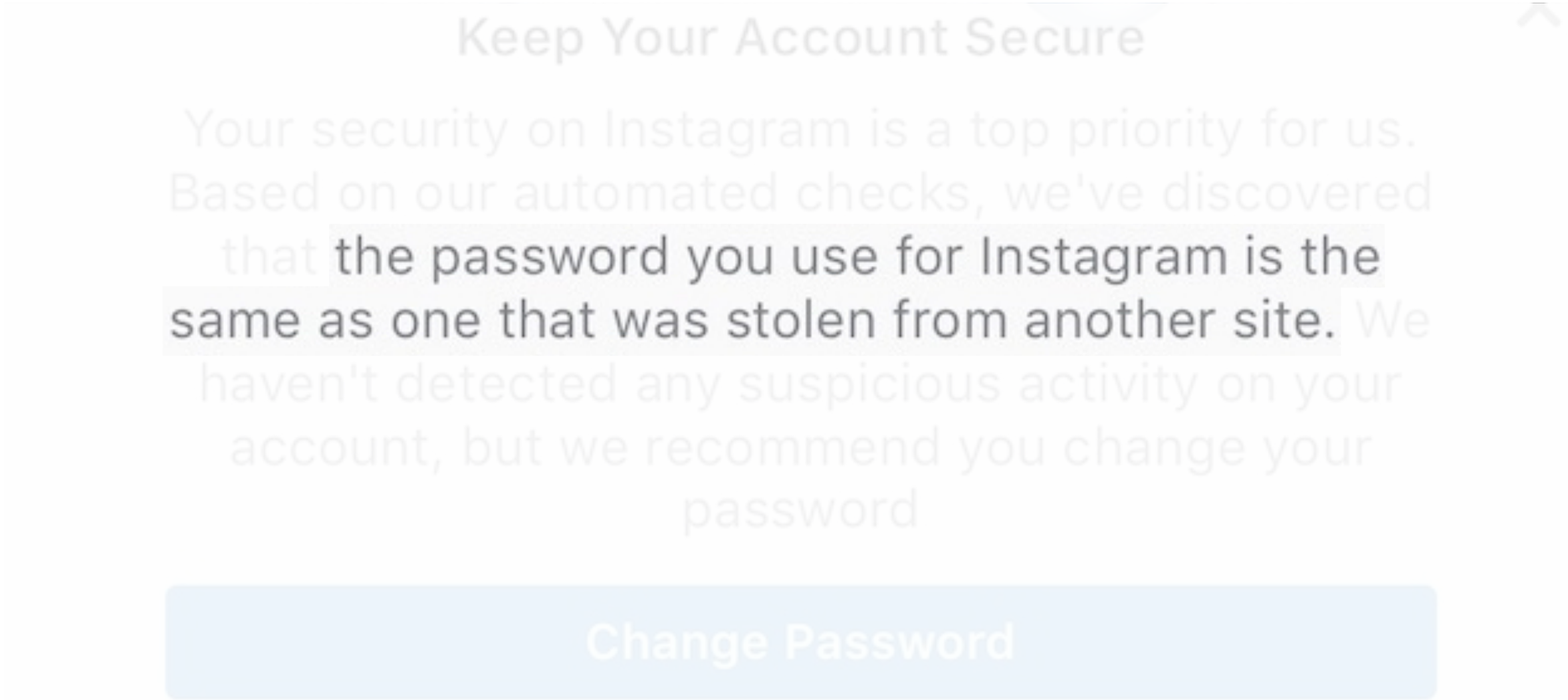
don’t mention password reuse

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

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

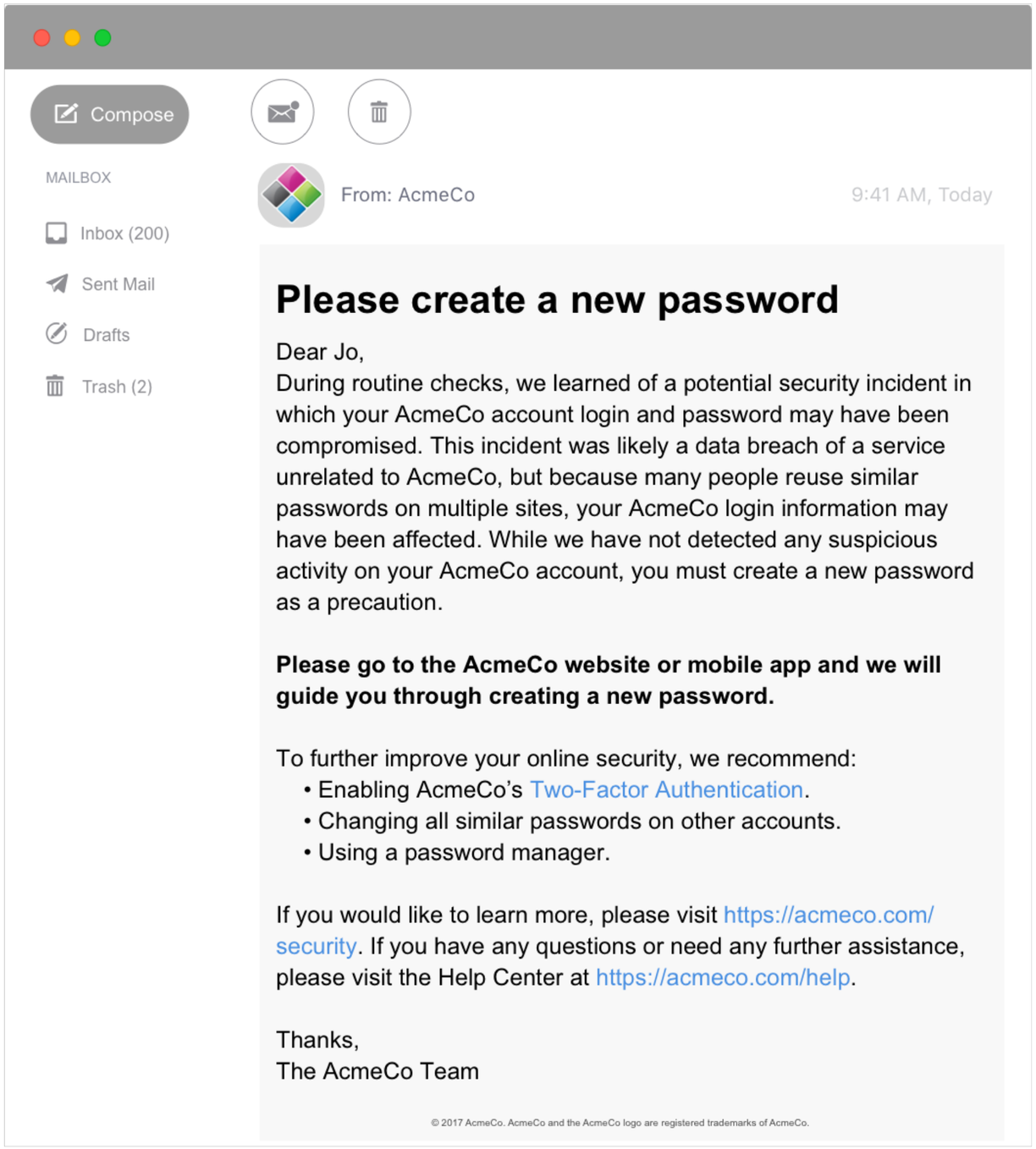
secure actions

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)

2

“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

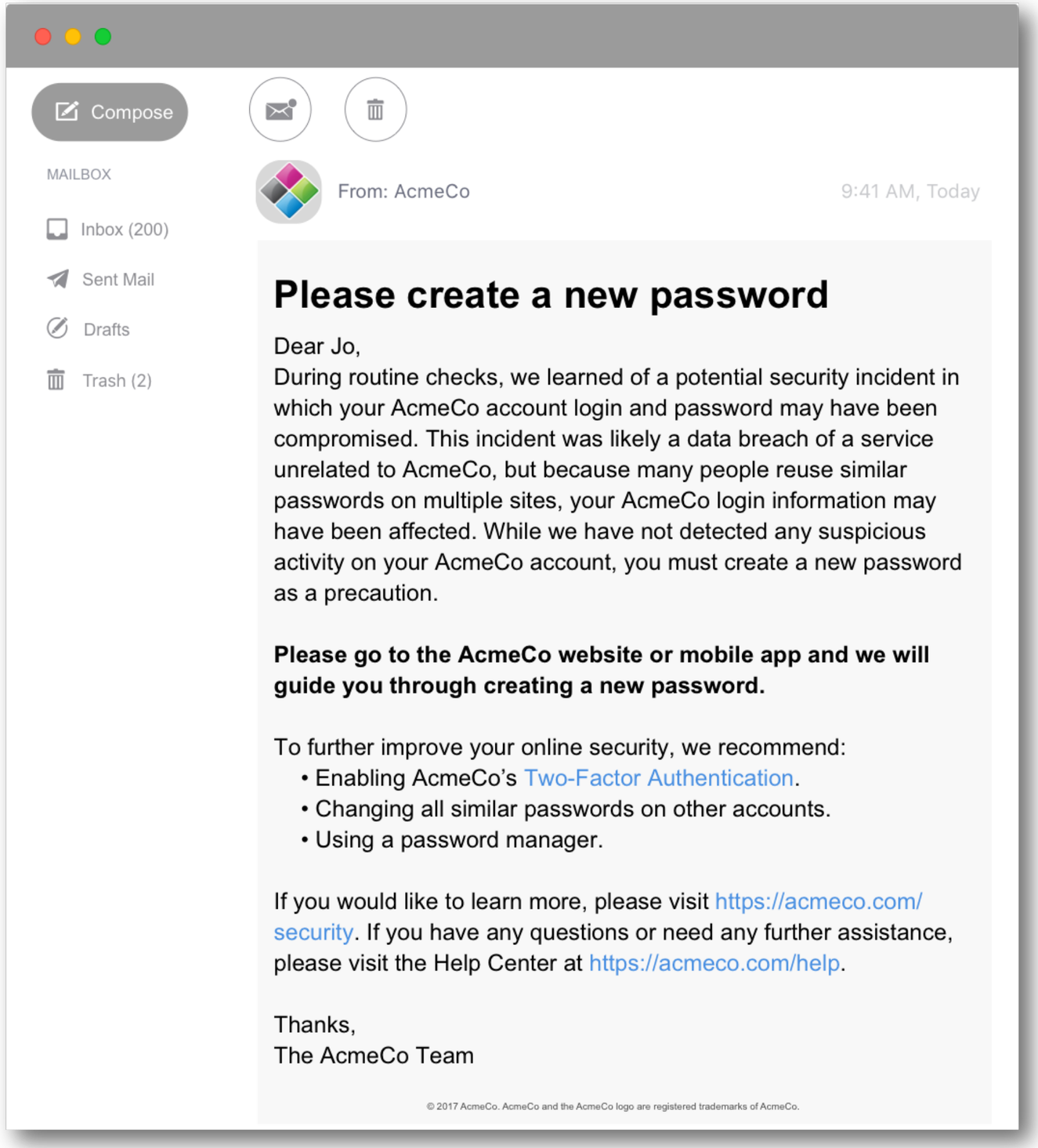
send via email + more immediate channel

name password reuse as root cause

force password reset

encourage 2FA and password managers

suggest unique passwords for other accounts

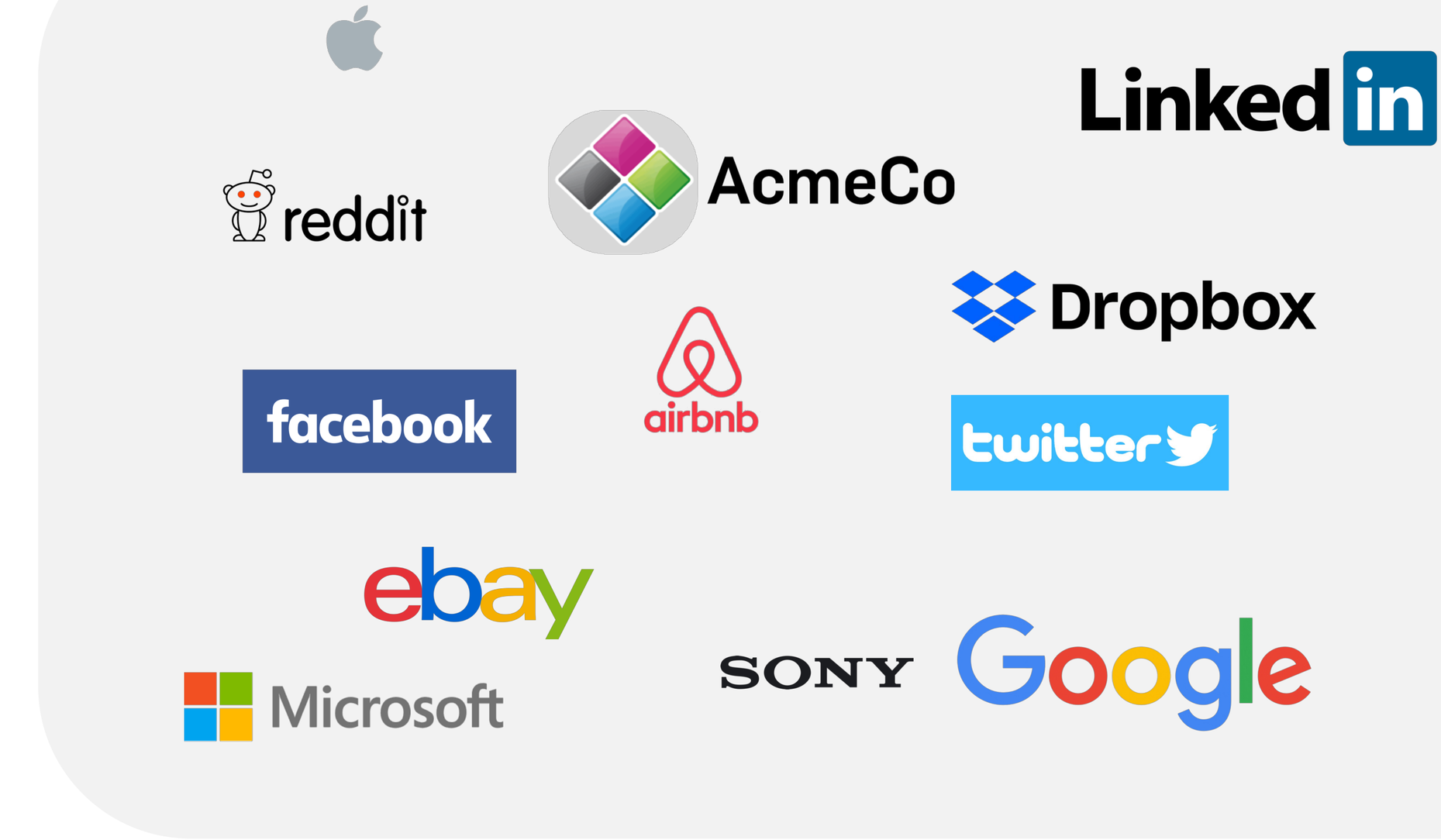

Compose
MAILBOX
Inbox (200)
Sent Mail
Drafts
Trash (2)
From: AcmeCo
9:41 AM, Today
Please create a new password
Dear Jo,
During routine checks, we learned of a potential security incident in which your AcmeCo account login and password may have been compromised. This incident was likely a data breach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

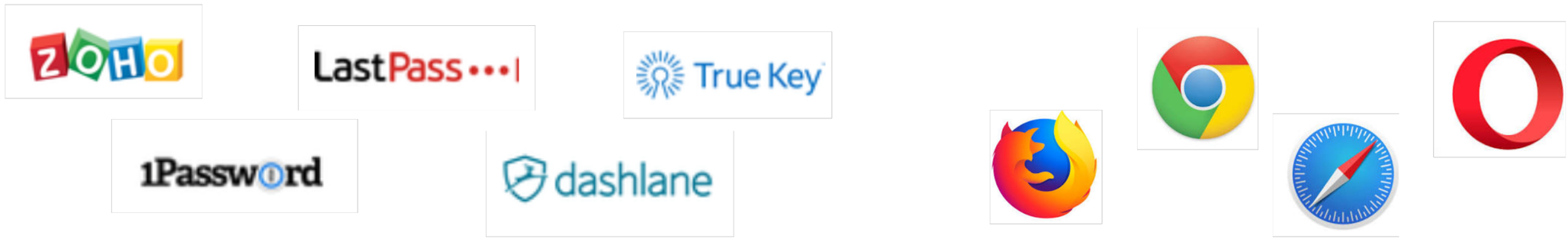
conclusion

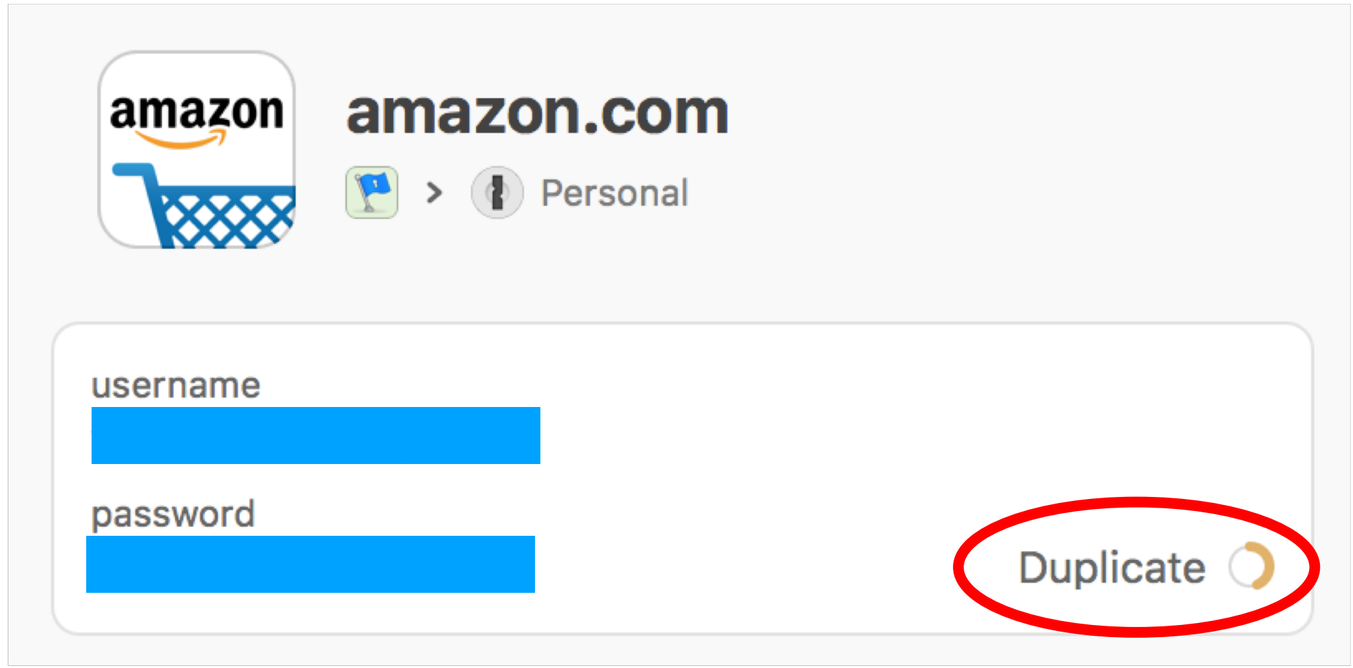
1. formative, systematic study of password-reuse notifications

2. developed best practices

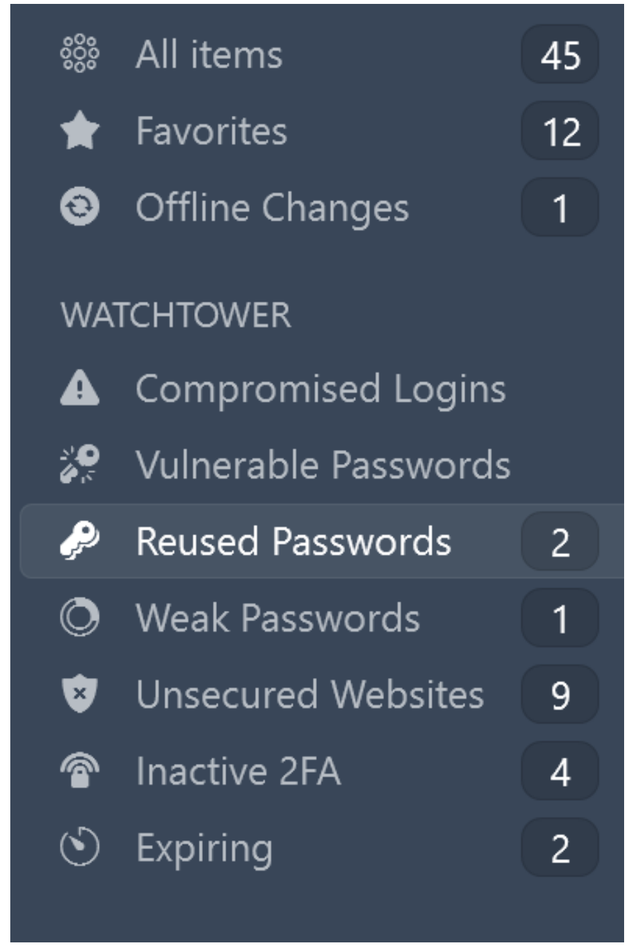
3. future work should study novel notifications

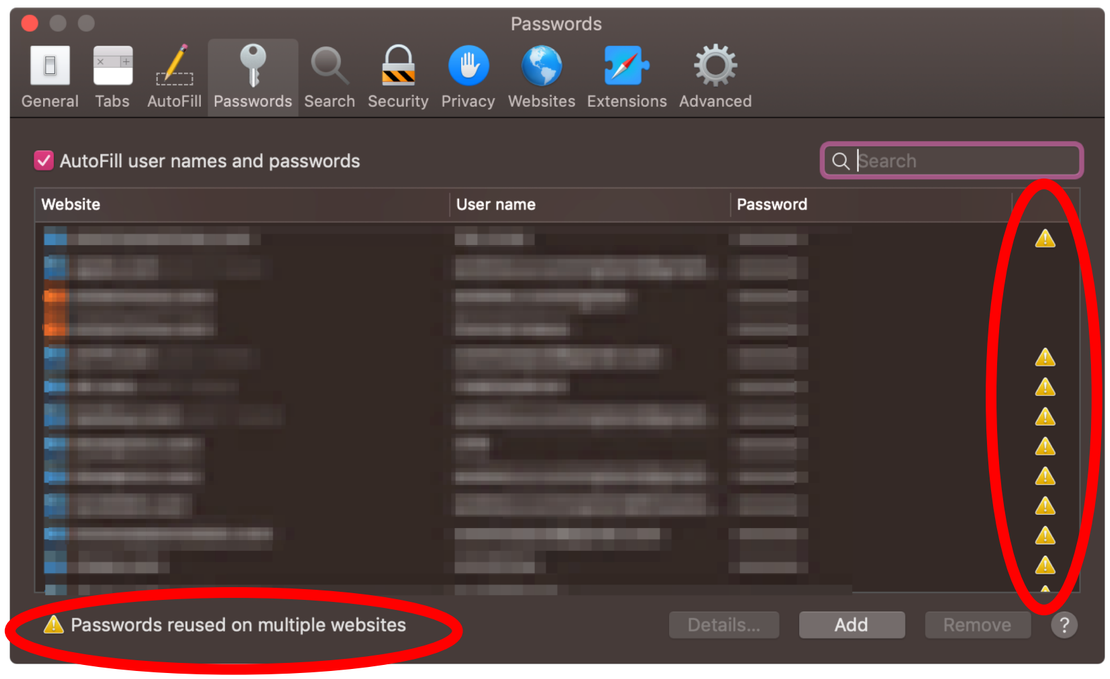

reddit
AcmeCo
LinkedIn
Dropbox
facebook
airbnb
twitter
ebay
Microsoft
SONY
Google


ZOHO
LastPass
True Key
1Password
dashlane



1Password





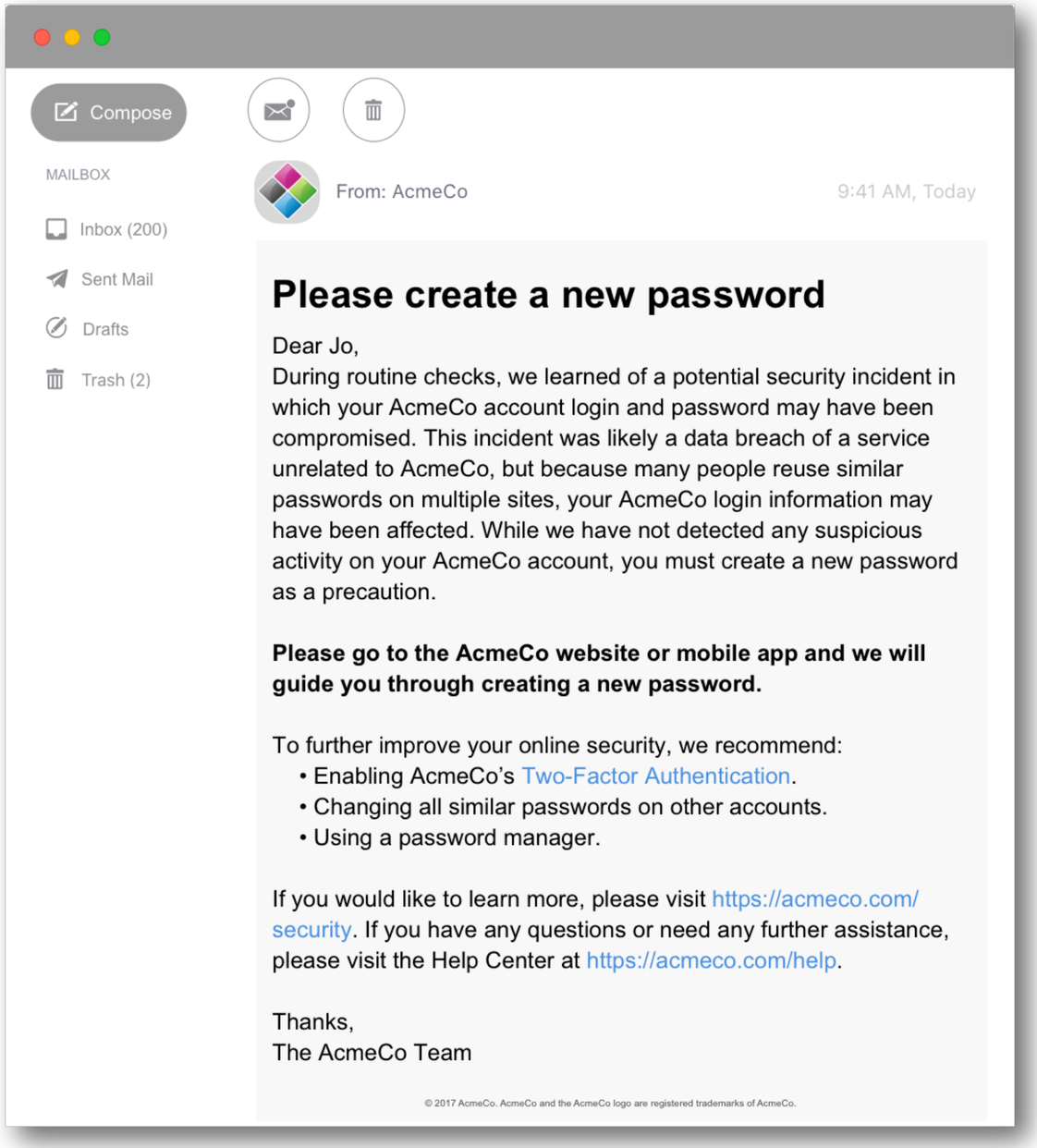
macOS Mojave, Safari 12

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



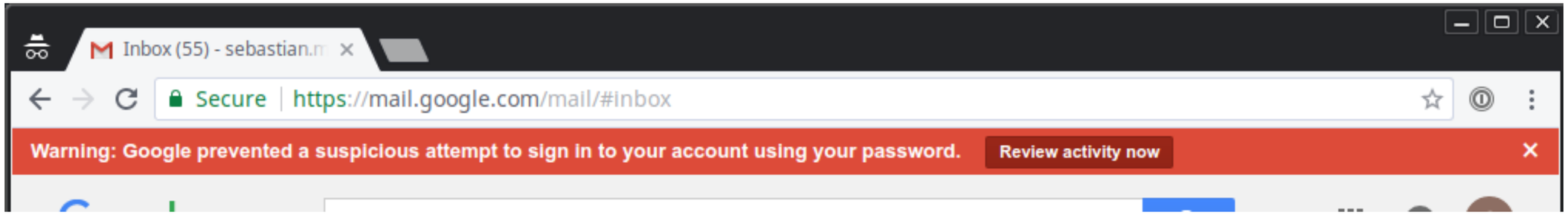
Designing Password-Reuse Notifications

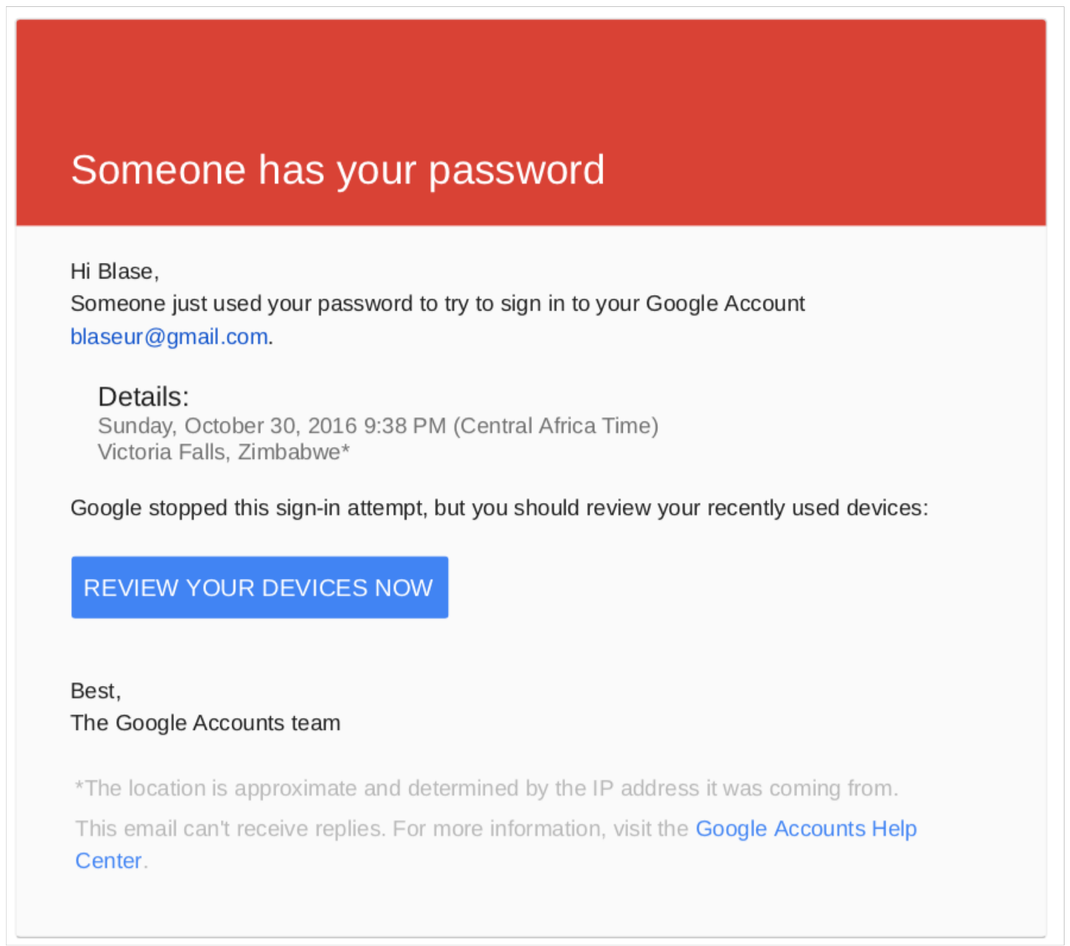
Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, Blase Ur

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

extra slides

representative notifications





representative notifications

NETFLIX

Dear Sam,

We have detected a suspicious sign-in to your Netflix account. Your Netflix account may have been compromised by a website or a service not associated with Netflix. Just to be safe and prevent any further unauthorized access of your account, we've reset your password.

Please visit the login page at https://www.netflix.com/LoginHelp or type www.netflix.com into your browser, click on “sign in”, and then click “forgot your email or password.” Follow the instructions to reset your password. You will need to use your new password to sign in to Netflix on your devices.

We recommend that you also change your password on any other websites where you may have used the same password. We also want to assure you that your payment information is secure and does not need to be changed. We have more recommendations for how to keep your Netflix account secure in our Help Center.

If you have any questions or need further assistance, please visit the Help Center at https://help.netflix.com/help or call us at 1-866-579-7172.

–The Netflix Team

in

Kif Leswing

Hi Kif,

To make sure you continue having the best experience possible on LinkedIn, we're regularly monitoring our site and the Internet to keep your account information safe.

We've recently noticed a potential risk to your LinkedIn account coming from outside LinkedIn. Just to be safe, you'll need to reset your password the next time you log in.

Here's how:

1. Go to the LinkedIn website.
2. Next to the password field, click the "Forgot your password" link, and enter your email address.
3. You'll get an email from LinkedIn asking you to click a link that will help you reset your password.
4. Once you've reset your password, a confirmation email will be sent to the confirmed email addresses on your account.

Thanks for helping us keep your account safe,
The LinkedIn Team

Someone May Have Accessed Your Account

Recently, there was a security incident on another website unrelated to Facebook. Facebook was not directly affected by the incident, but your Facebook account is at risk because you were using the same password in both places.

To secure your account, you'll need to answer a few questions and change your password. For your protection, no one can see you on Facebook until you finish.

Continue

“password-reuse notifications”

About any situation that could have been caused by password reuse.

Authentication and Access Control CHI 2017, May 6–11, 2017, Denver, CO, USA

I'm too Busy to Reset my LinkedIn Password: On the Effectiveness of Password Reset Emails

Jun Ho Huh
Honeywell ACS Labs
junho.huh@honeywell.com

Hyoungshick Kim
Sungkyunkwan University
hyoung@skku.edu

Swathi S.V.P. Rayala
Oregon State University
rayalas@oregonstate.edu

Rakesh B. Bobba
Oregon State University
rakesh.bobba@oregonstate.edu

Konstantin Beznosov
University of British Columbia
beznosov@ece.ubc.ca

REAL-LIFE

46%
reset LinkedIn password

33%
changed passwords for accounts with similar passwords

SELF-REPORT

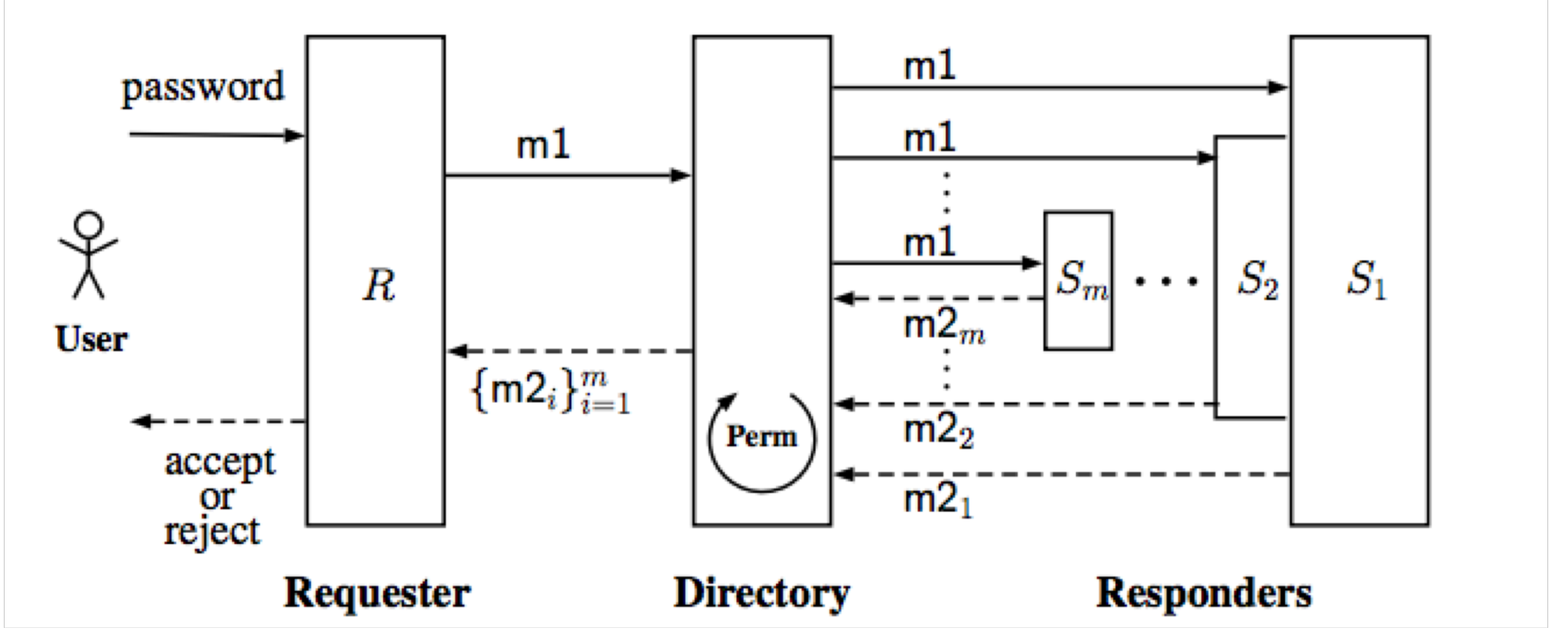
90%
said would reset AcmeCo password

35%
said would change passwords if same/similar

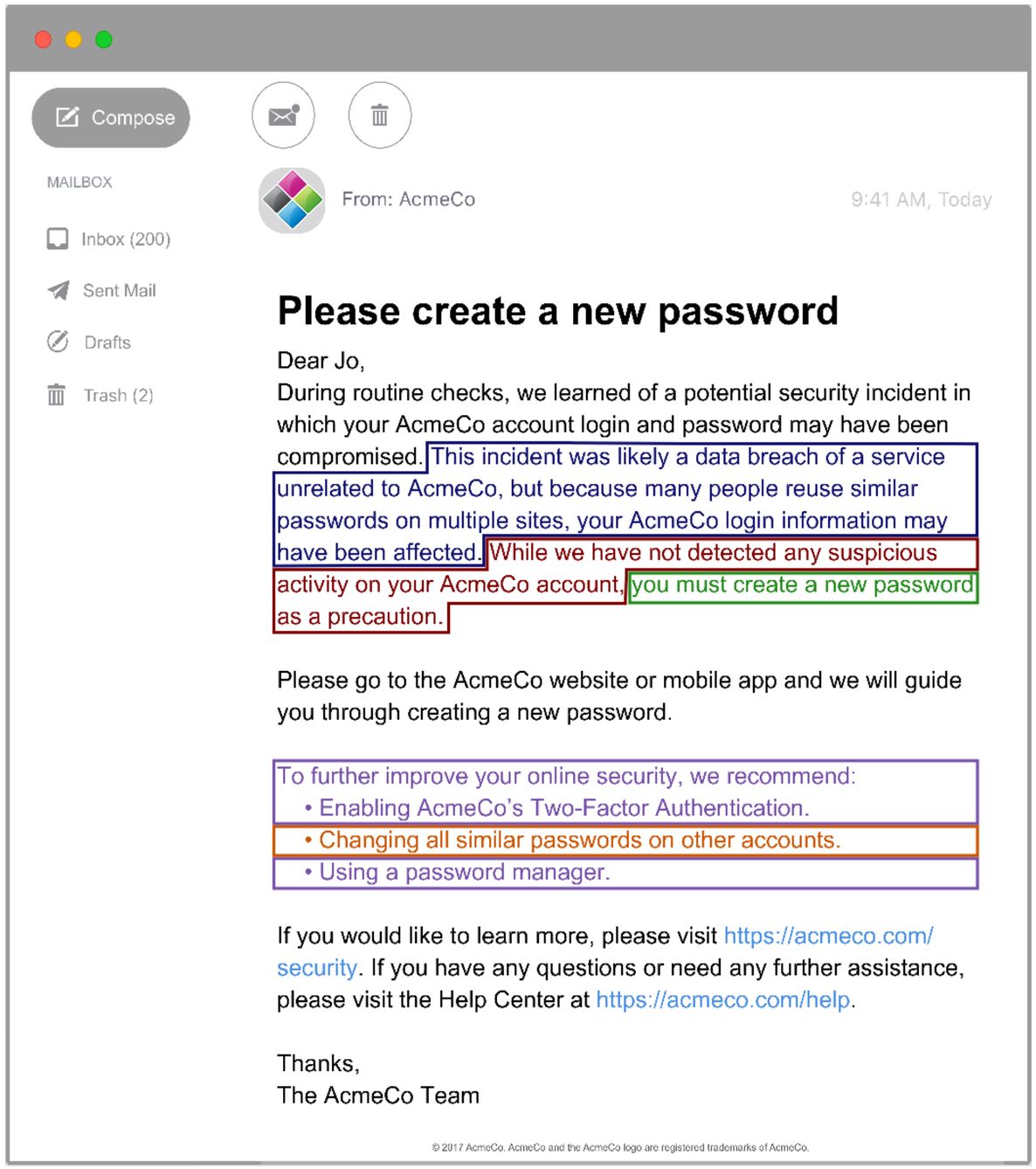
How to End Password Reuse on the Web

Ke Coby Wang
Department of Computer Science
University of North Carolina at Chapel Hill
kwang@cs.unc.edu

Michael K. Reiter
Department of Computer Science
University of North Carolina at Chapel Hill
reiter@cs.unc.edu

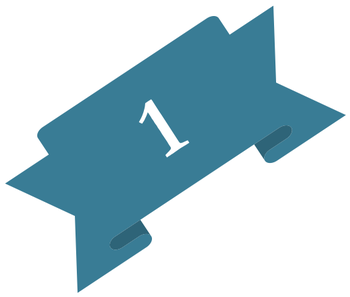


study 2 variations



Delivery Medium	
model	Delivered by email
inApp	Mobile in-app
mobile	Mobile push notification and in-app
Incident	
model	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.
usBreach	This incident was likely a data breach of one of our services.
vagueCause	—
Account Activity	
model	While we have not detected any suspicious activity on your AcmeCo account, …as a precaution.
suspicious	Because we have detected suspicious activity on your AcmeCo account, …
omitActivity	—
Remediation	
model	…you must create a new password …
recommend	…we recommend that you create a new password.
Other Accounts	
model	Change all similar passwords on other accounts.
noOthers	—
Extra Actions	
model	To further improve your online security, we recommend: • Enabling AcmeCo's Two-Factor Authentication. • Using a password manager.
noExtras	—

covariates



- CS literacy
- Gender
- ...

???