

“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**



Security, Usability, & Privacy  
Education & Research

# use unique passwords

Next

## You'll need a password

Make your password unique.

Password

---

# Booking.com



# PayPal



American Airlines

The American Airlines logo features the airline's name in a dark blue sans-serif font next to a red and blue stylized tail logo.

reddit

The Reddit logo is a white cartoon alien head with orange eyes, positioned next to the word "reddit" in a black sans-serif font.

Taobao.com

The Taobao logo consists of the Chinese characters "淘宝网" in orange, with "Taobao.com" in a smaller, gray sans-serif font below it.

Baidu 百度

The Baidu logo features a large blue paw print icon next to the Chinese characters "百度" in red, with "Baidu" in a bold red sans-serif font above it.

WELLS FARGO

The Wells Fargo logo is a red square containing the words "WELLS" and "FARGO" in yellow, with a small registered trademark symbol.

1&1

The 1&1 logo is a blue square containing the white text "1&1".

Dropbox

The Dropbox logo features a blue diamond shape divided into six triangles, with the word "Dropbox" in a black sans-serif font to its right.

facebook

The Facebook logo is a blue rounded rectangle containing the white word "facebook".

airbnb

The Airbnb logo consists of a red abstract house-like shape with the word "airbnb" in red lowercase letters below it.

twitter

The Twitter logo is a light blue rounded rectangle containing the white word "twitter" and a small white bird icon.

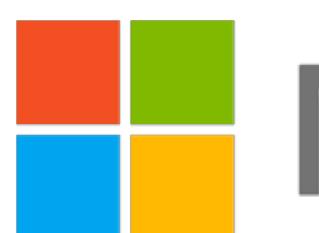
Adobe

The Adobe logo is a red square containing a white stylized letter "A".

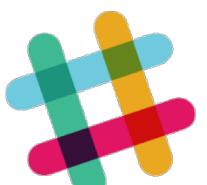
ebay

The eBay logo features the word "ebay" in a colorful, slanted sans-serif font.

YouTube

The YouTube logo is a red rounded rectangle containing the white word "YouTube".

Microsoft



slack

SONY

Google

The Google logo features the word "Google" in its signature multi-colored, rounded sans-serif font.

# “use a password manager!”

The screenshot shows the 1Password application interface. On the left, there's a sidebar with navigation links: All Vaults (7 Vaults), All Items (77), Favourites, WATCHTOWER, and CATEGORIES (Logins, Secure Notes, Credit Cards, Identities, Bank Accounts, Driver Licenses, Passports). The main area displays a list of 77 items sorted by title. The items include:

- AgileBits Corporate Card (AMEX icon)
- AgileBits Forum (Icon with star)
- AgileBits Office Wi-Fi (Icon with star)
- Alfred (Icon with magnifying glass)
- Amazon (Amazon icon)
- Apple ID (iCloud) (Selected item, highlighted in blue)
- AWS (AWS icon)
- CBC.ca (CBC logo icon)
- D

The selected item, "Apple ID (iCloud)", has a detailed view on the right. It shows the following fields:

username	wendy.c.appleseed@gmail.com
password	*****
Apple ID	<a href="https://appleid.apple.com/#!&amp;page=signin">https://appleid.apple.com/#!&amp;page=signin</a>
iCloud	<a href="https://www.icloud.com">https://www.icloud.com</a>
<b>SECURITY</b>	
best friend	*****
parents city	*****
mother's maiden	*****

Each security field is marked with a "Fantastic" rating and a green circle.

# people reuse passwords

Booking.com

R0cky!14



reddit

R0cky!17

淘宝网  
Taobao.com

American Airlines

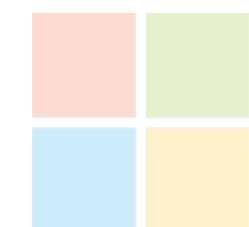


facebook

R0cky!17

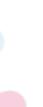


123456



Microsoft

Rocky!16



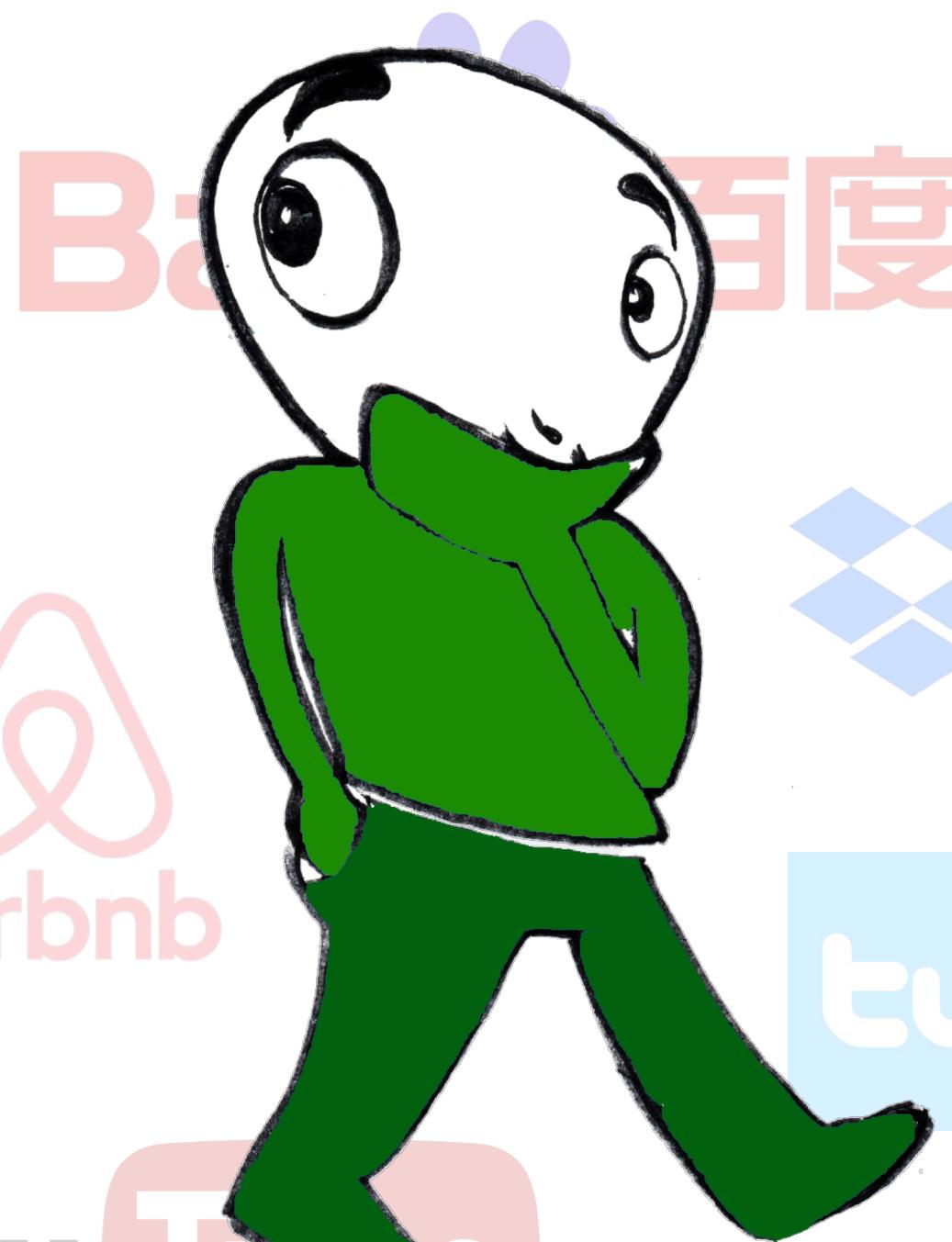
slack

SONY



Google

R0cky!17



PayPal

WELLS  
FARGO

1&1

Dropbox

R0ckyBox

twitter

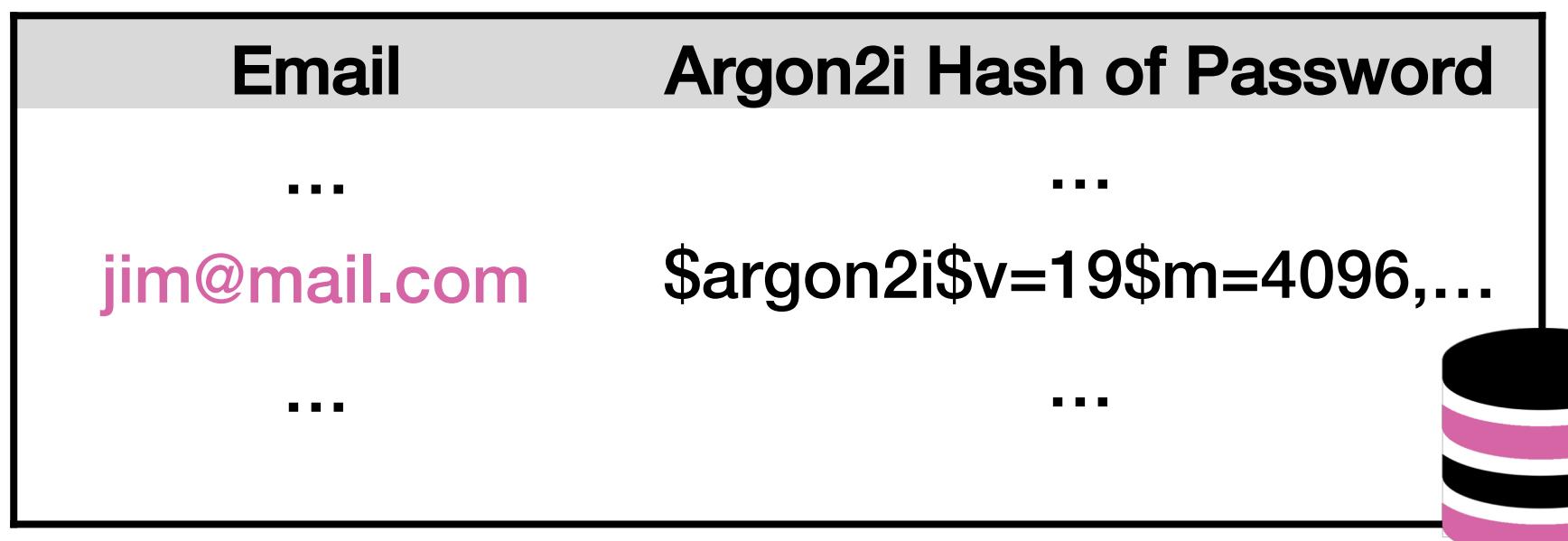
R0cky!17



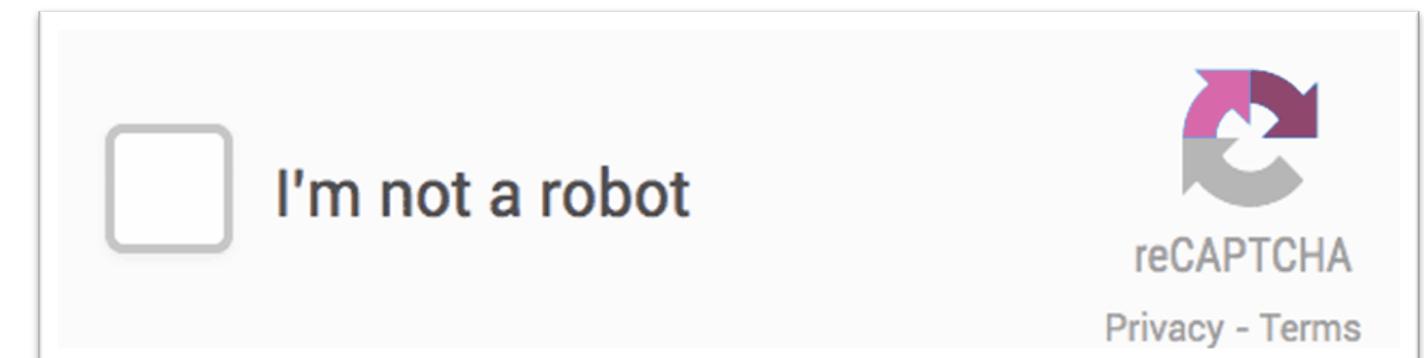
Spotify



## Memory-Hard Hash Function



## Rate-Limiting Guessing



Email

Argon2i Hash of Password

...

jim@mail.com

...

\$argon2i\$v=19\$m=4096,...

...

## Password Strength Meter



Username

Password

 acmccs18

Show Password & Detailed Feedback

Your password could be better.

- Consider inserting digits into [\(Why?\)](#) the middle, not just at the end
- Make your password longer [\(Why?\)](#) than 8 characters
- Consider using 1 or more [\(Why?\)](#) symbols

A better choice: \a#D18cmccs

[How to make strong passwords](#)



AcmeCo

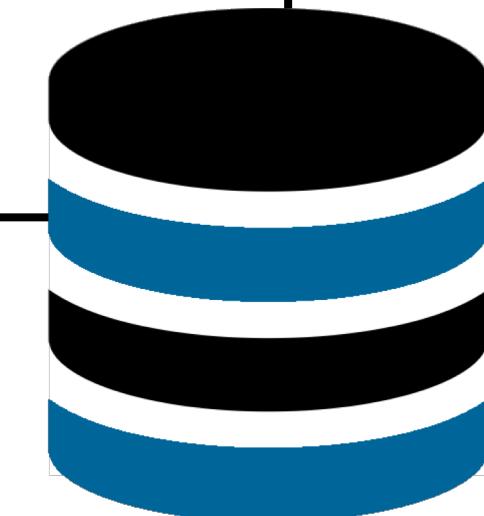


LinkedIn





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
...	...



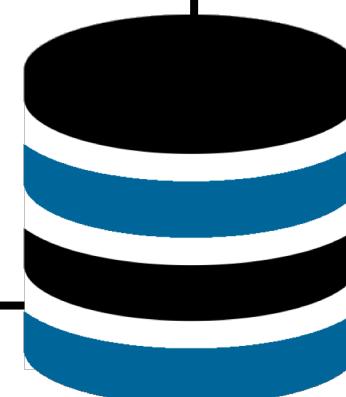
# crack all the things!



```
Bash
$> hashcat -m 100 -a0 $TARGET $DICT
123456
Password
R0cky!17
Football!17
CanadaRocks!
```



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

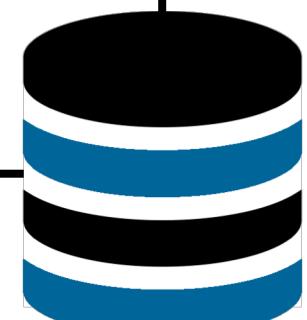
Email	Argon2i Hash of Password
...	...
jim@mail.com	\$argon2i\$v=19\$m=4096,...
...	...



1 guess is  
enough!

Linked in

Email	Cracked SHA-1 Hashes
jane@aol.com	123456
jessey@gmx.net	5baa61e4c9b93f3f068225
jenny@gmail.com	0b6
jim@mail.com	Canada4ever
john@hotmail.com	R0cky!17
...	HikingGuy89



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

Anatomy of a password disaster:  
Adobe's giant

RISK ASSESSMENT —

## How LinkedIn's password sloppiness hurts us all

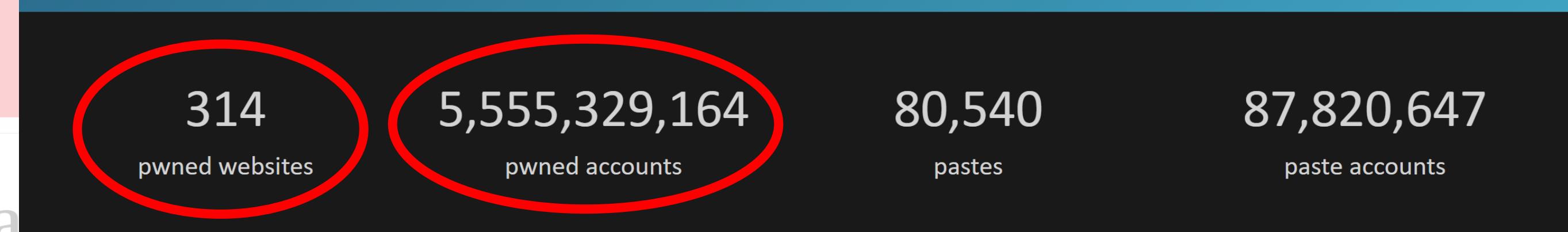
Check if you have an account that has been compromised in a data breach

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

**Facebook**

Facebook says it 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



### You Can Now Look Up Your Terrible 2006 MySpace Password

June 29, 2016 // 11:35 AM EST



Written by  
LORENZO FRANCESCHI-BICCIERAI  
STAFF WRITER



facebook

Connect with friends and the

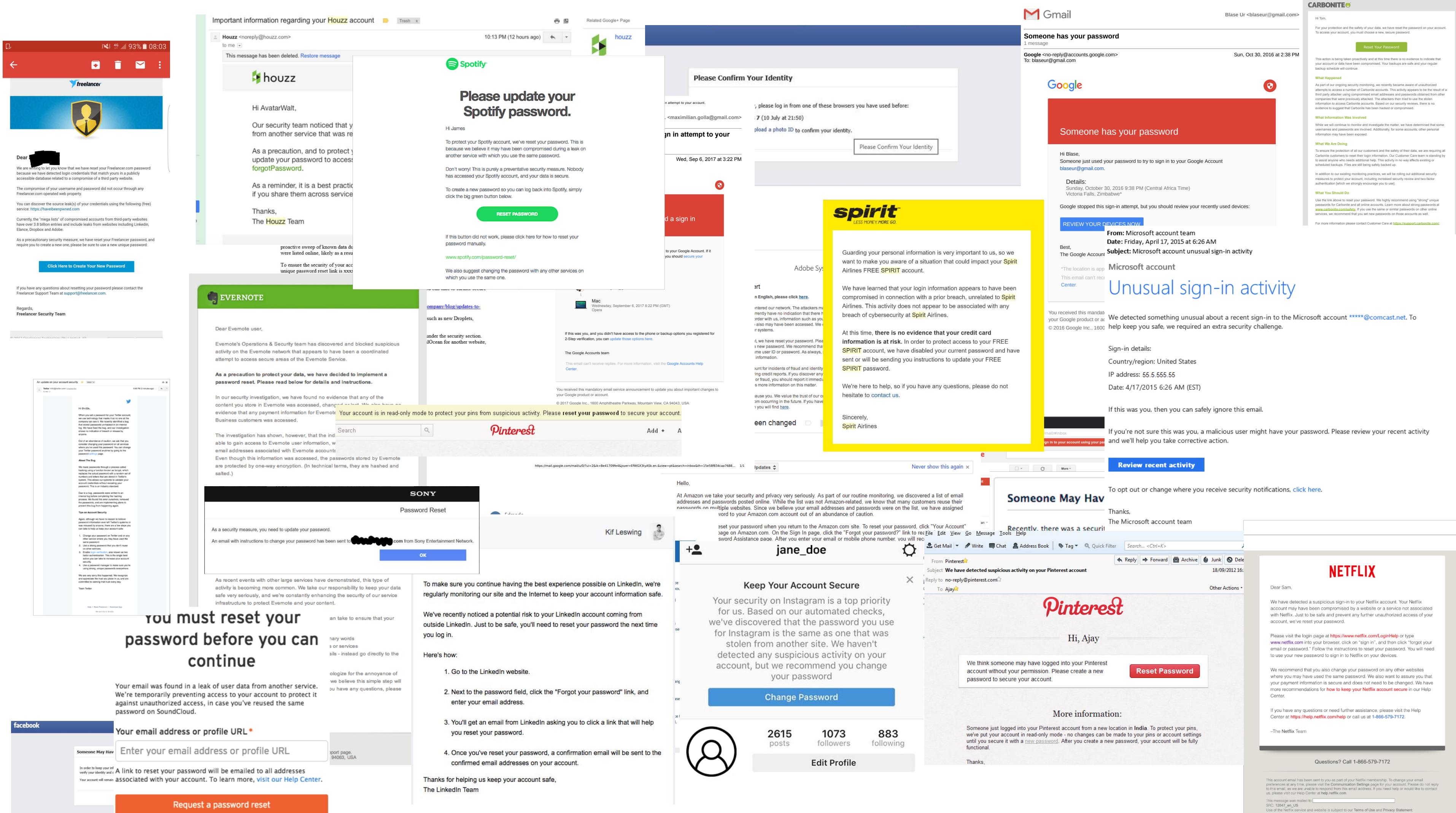
Sign Up

# black market monitoring

The screenshot shows a web browser window with a dark-themed interface, likely a Tor browser, displaying a listing on a black market. The title bar says "Listing". The address bar shows the URL [trdealmgm4uvn42g.onion/listing/3600](http://trdealmgm4uvn42g.onion/listing/3600). The header includes a welcome message "Welcome back, [REDACTED]", notification counts (0, 0, 0), a BTC balance of "BTC 0.0000", and links for "Home", "My RealDeal", "Support", and "Logout". A search bar contains the placeholder "I want to order ...".

The main content area shows a listing for "LinkedIn 167M" by user "peace\_of\_mind" (100.0%, Level 1 (14)). The price is listed as "0 5.0000 / BTC 5.0000" and is marked as "In stock". There is a dropdown menu for "Postage Option". To the right, there is a quantity selector set to "0" and a large red "Buy It Now" button. Below the listing, there are details: "Escrow" (Yes, escrow by RealDeal is available), "Class" (Digital), and "Ships From" (Worldwide). There are also "Favorite" and "Question" buttons.

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





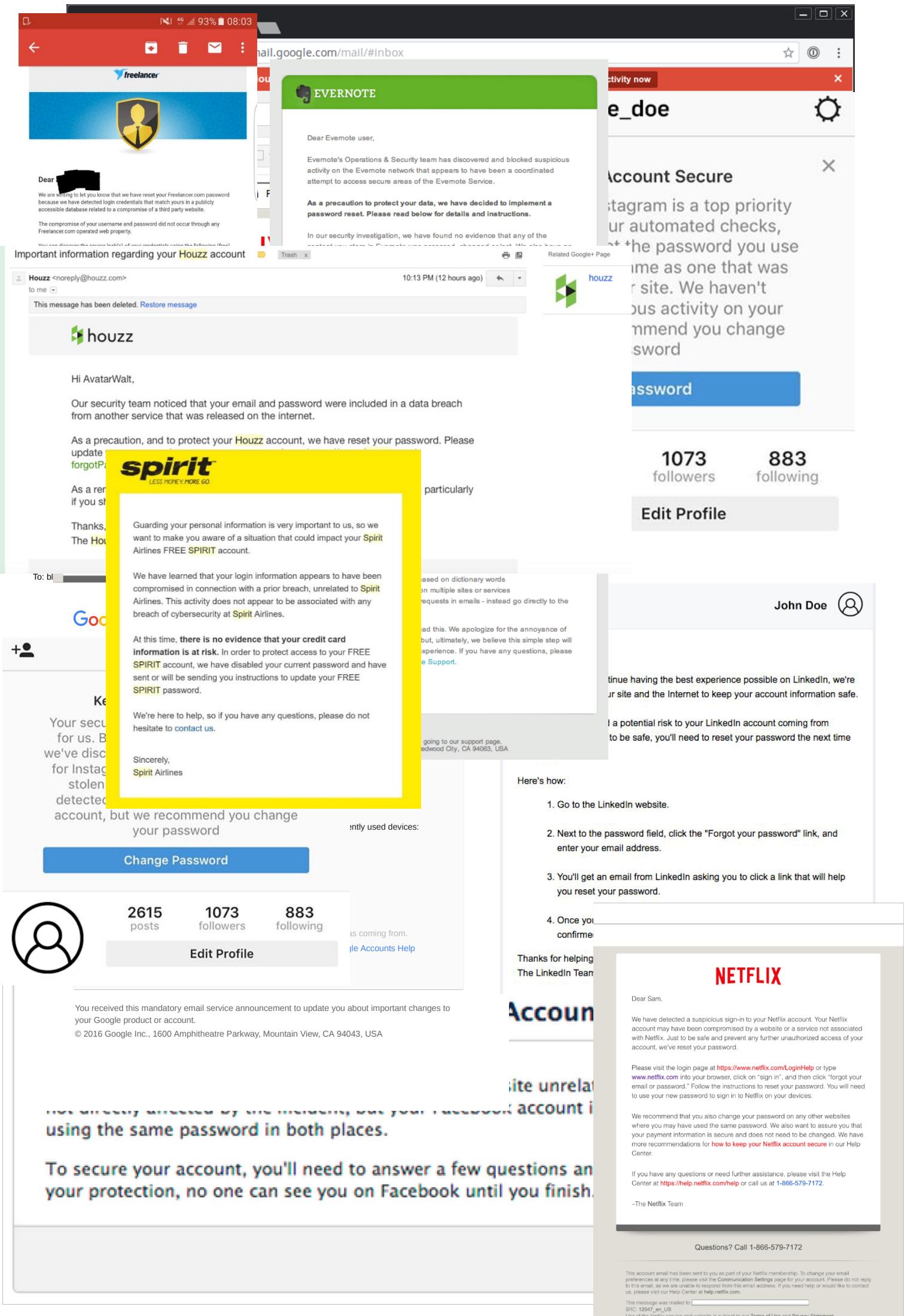
## Keep your account secure

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

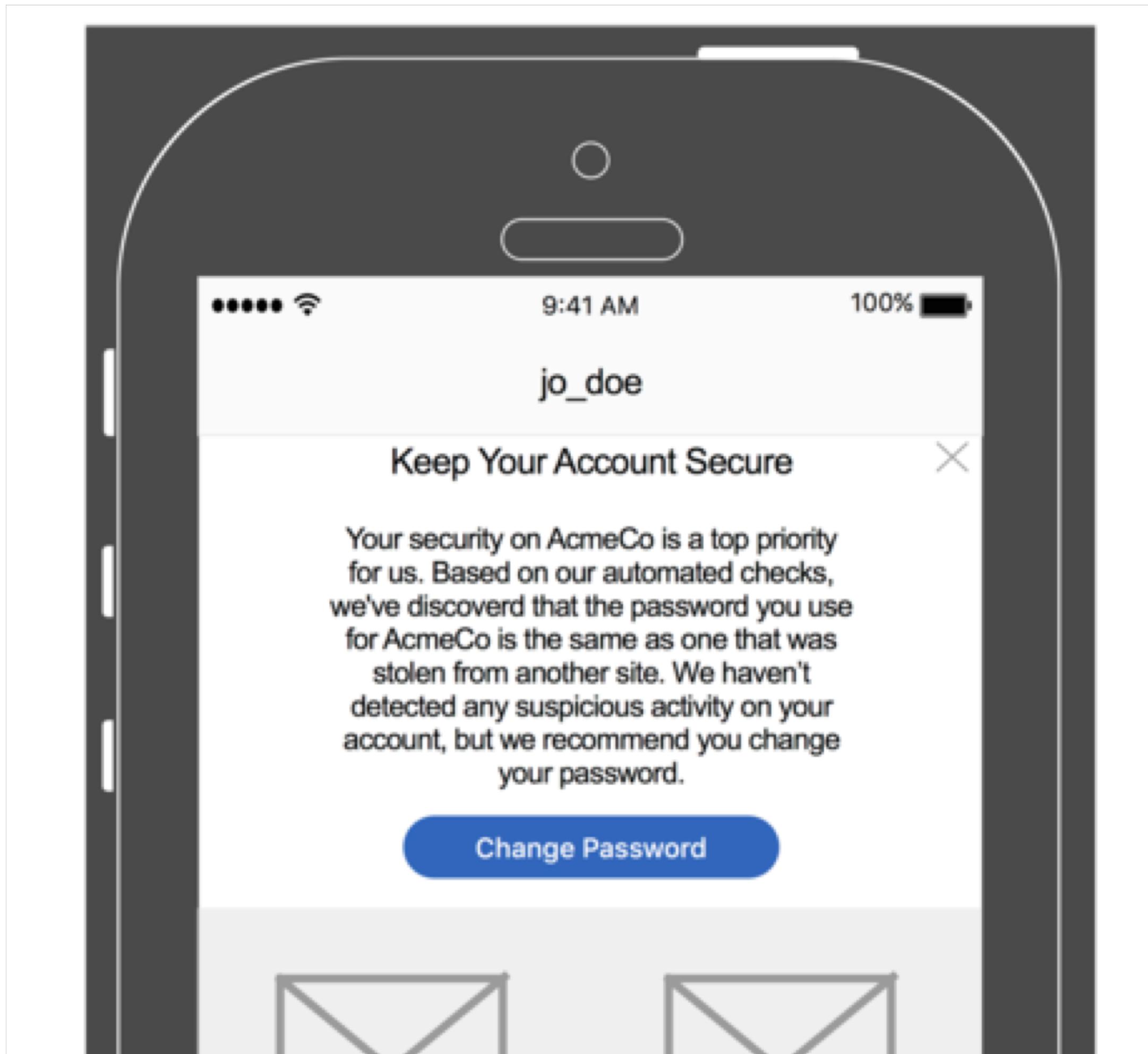
previously sent password-reuse notifications

## STUDY 2

individual components of password-reuse notifications

Imagine you have an  
important account with  
AcmeCo...

# AcmeCo notifications



# questions asked

notification  
understanding



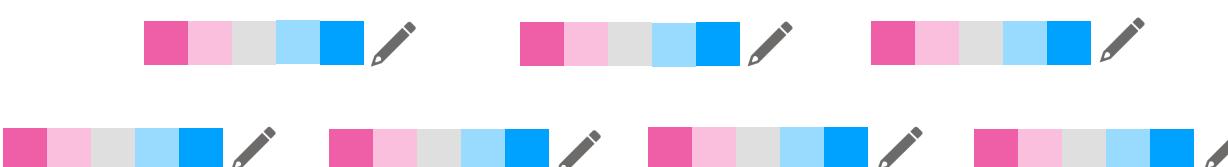
feelings



actions



perceptions



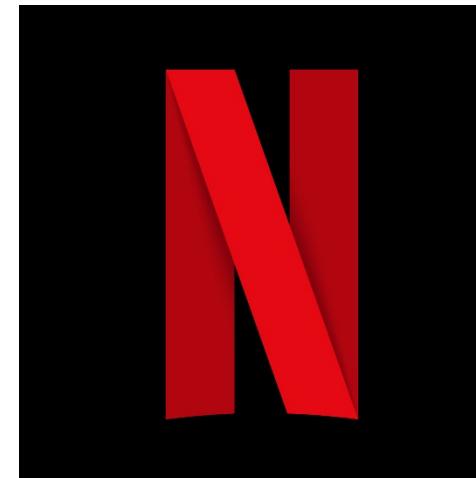
demographics

# survey setup

180 respondents

- Amazon MTurk
- 15 mins
- Compensated \$2.50

6 conditions



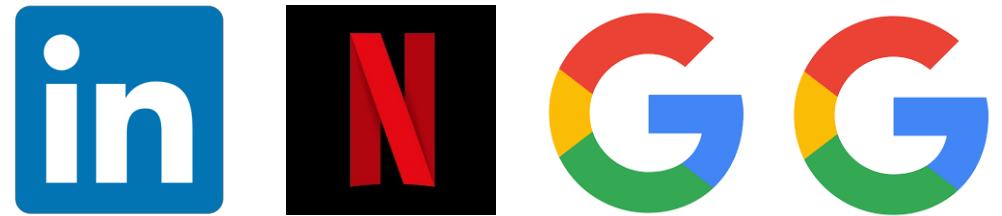
# notifications were concerning and a priority



# Why did you receive this notification?

**60%** hacked account

**21%** data breach



don't mention  
password  
reuse

0 - 4%  
respondents

listed password reuse as a cause



allude to  
password reuse

48 - 56%  
respondents



## 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](#)

*“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

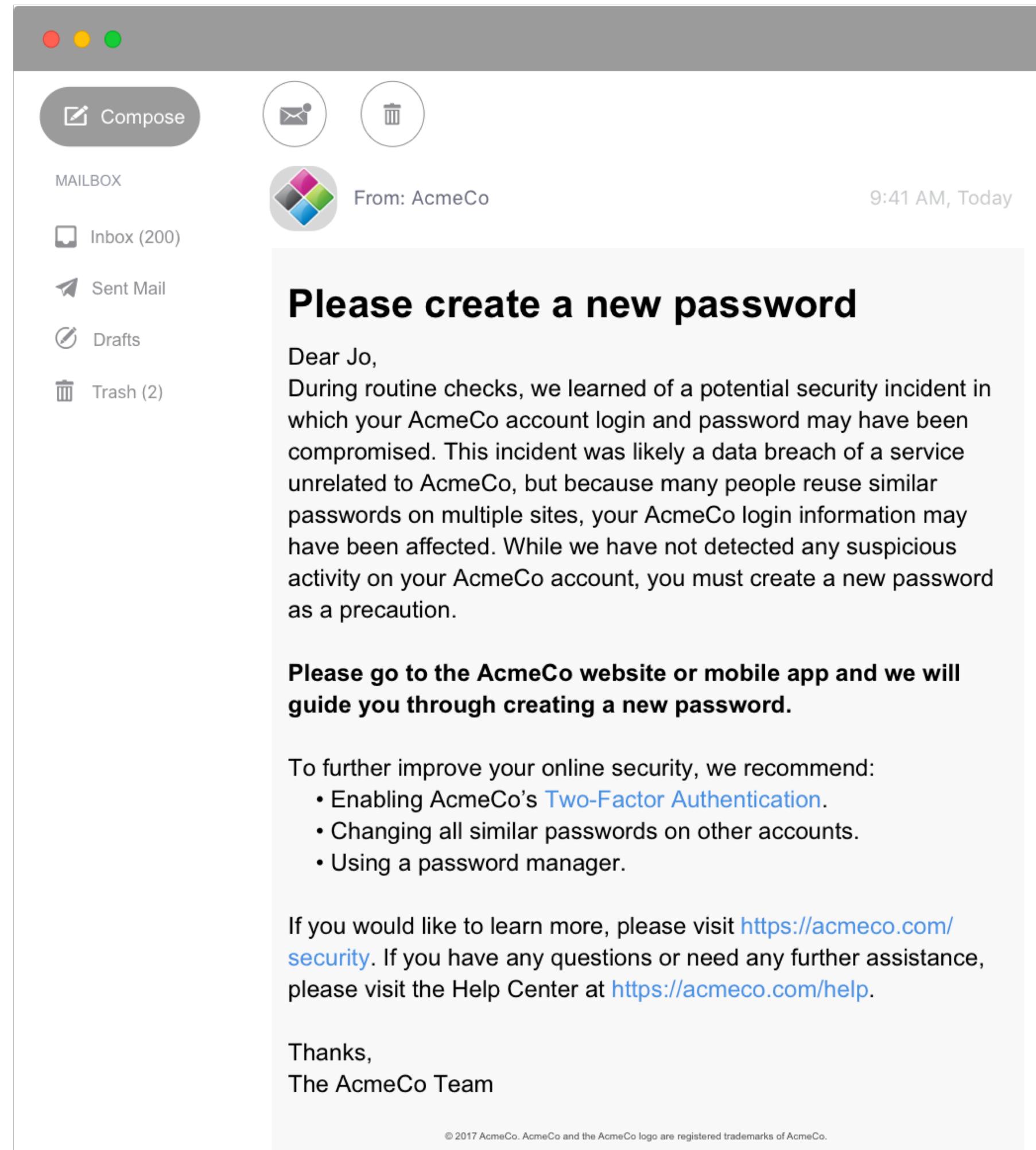
sufficient  
background

secure  
actions

legitimate

trust

# our model notification



# 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

# What would you do about your AcmeCo password?

Keep it the same

6%

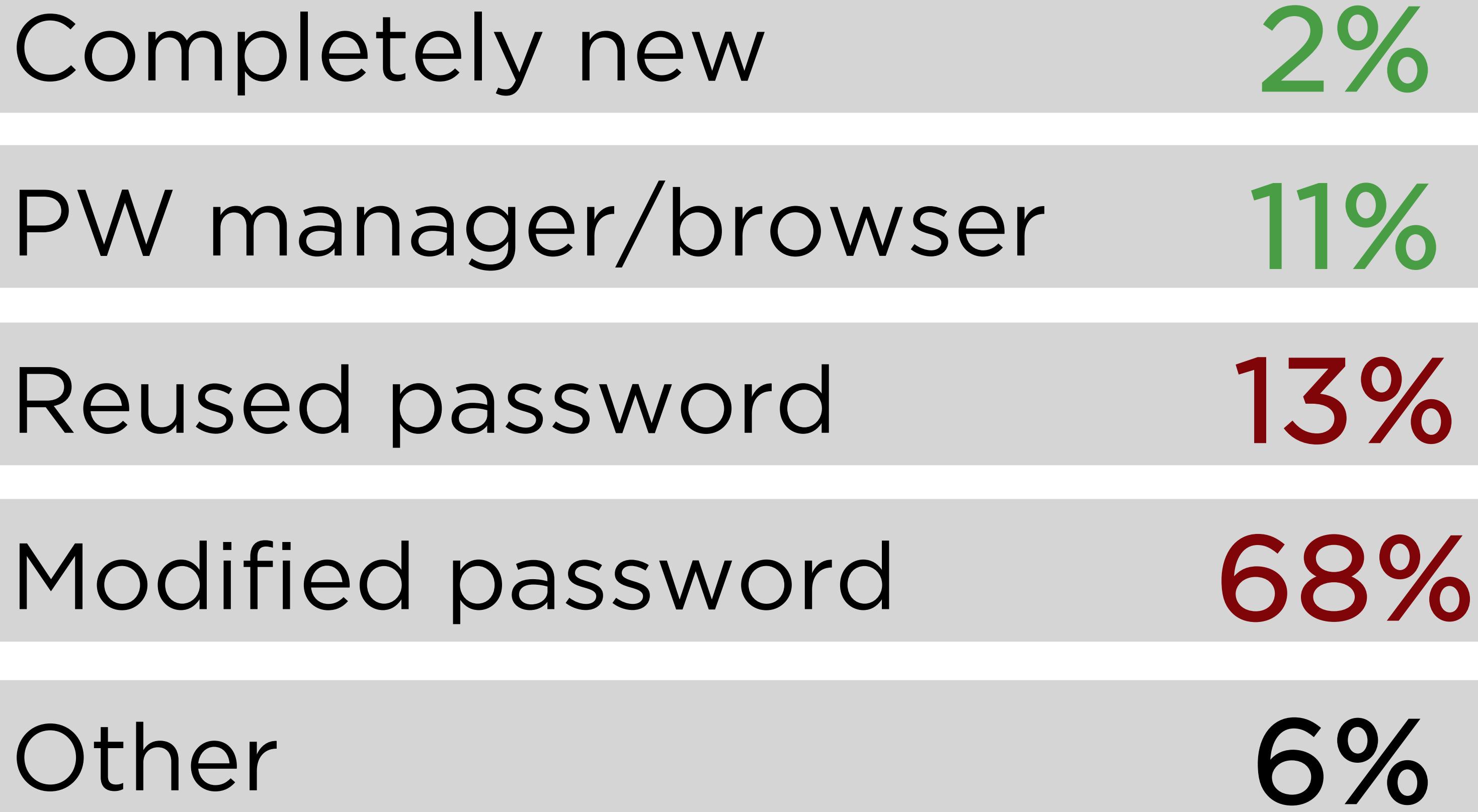
Change it

90%

Don't know

3%

# What would your new password be?



*“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)*

*“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

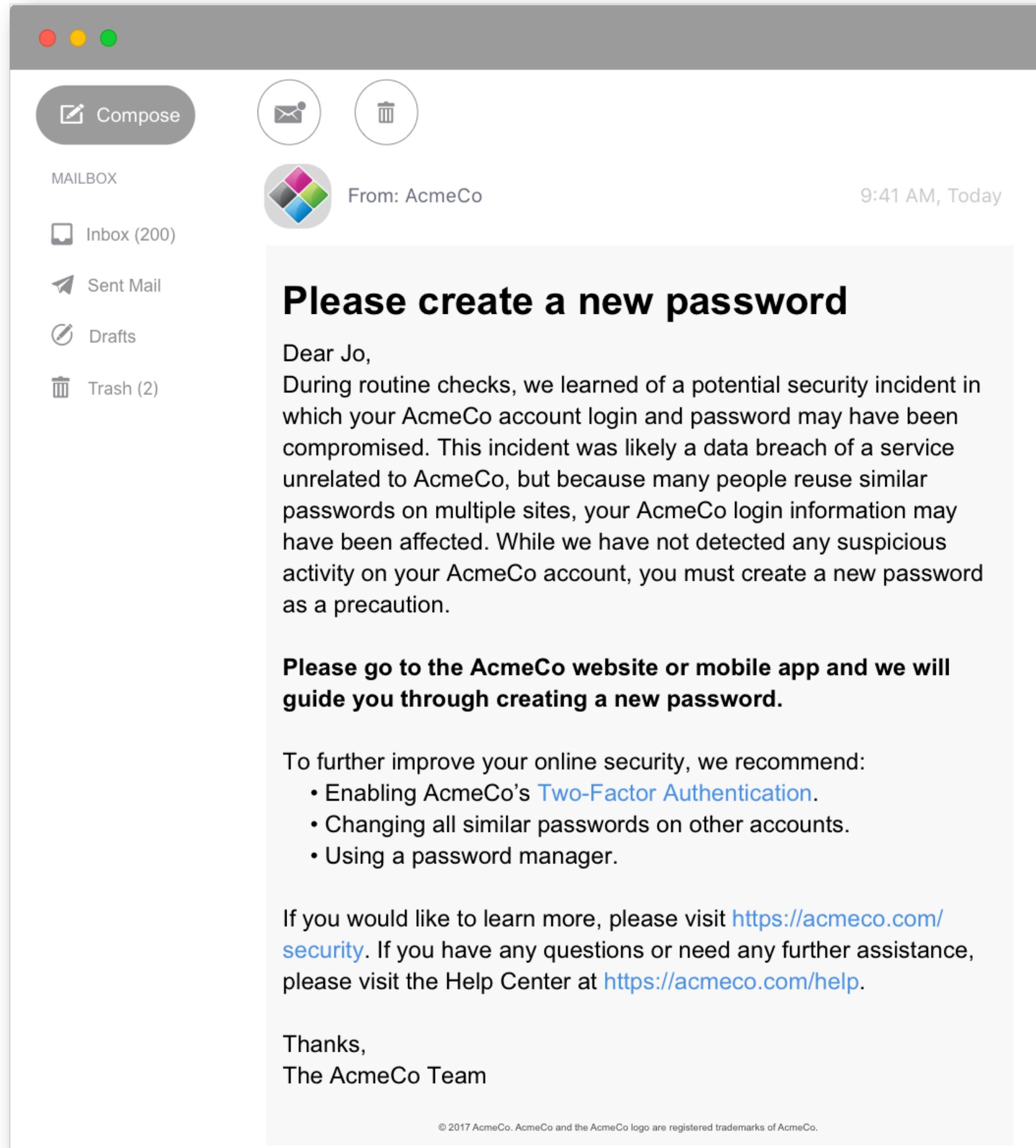
send via email + more immediate channel

name password reuse as root cause

force password reset

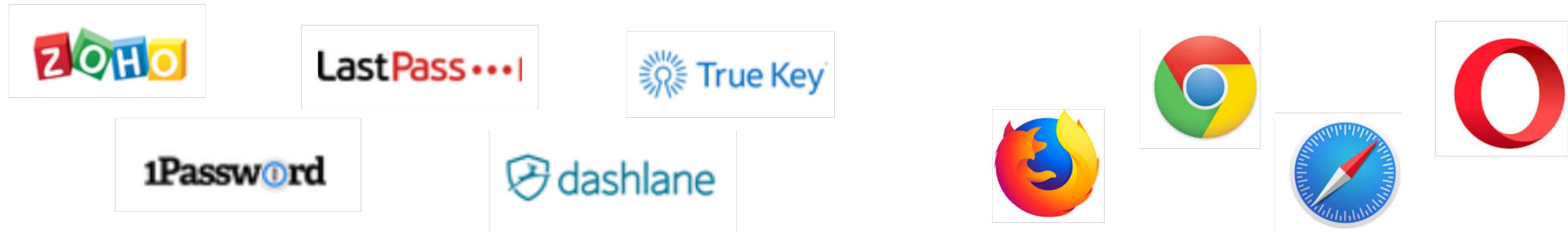
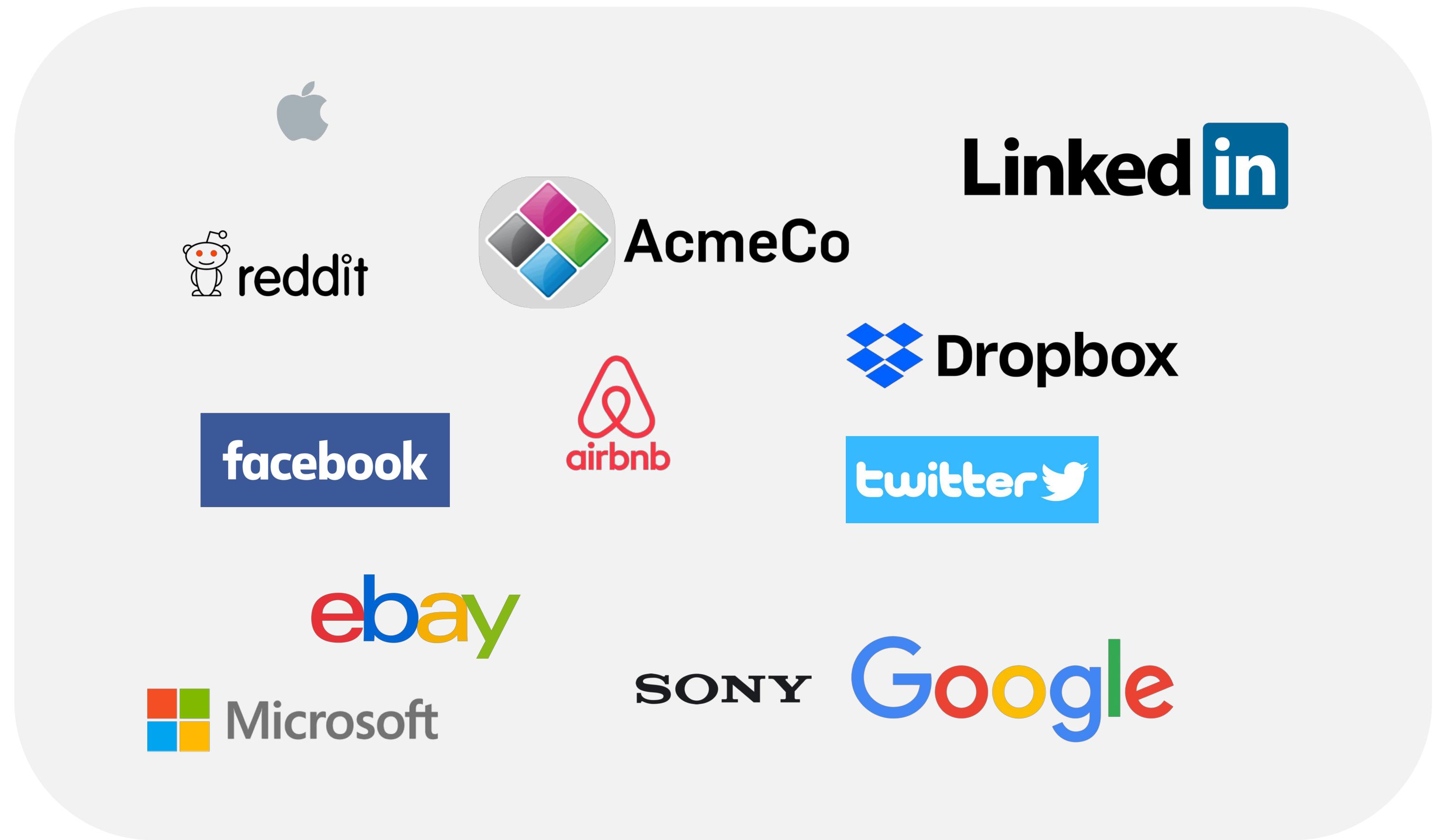
encourage 2FA and password managers

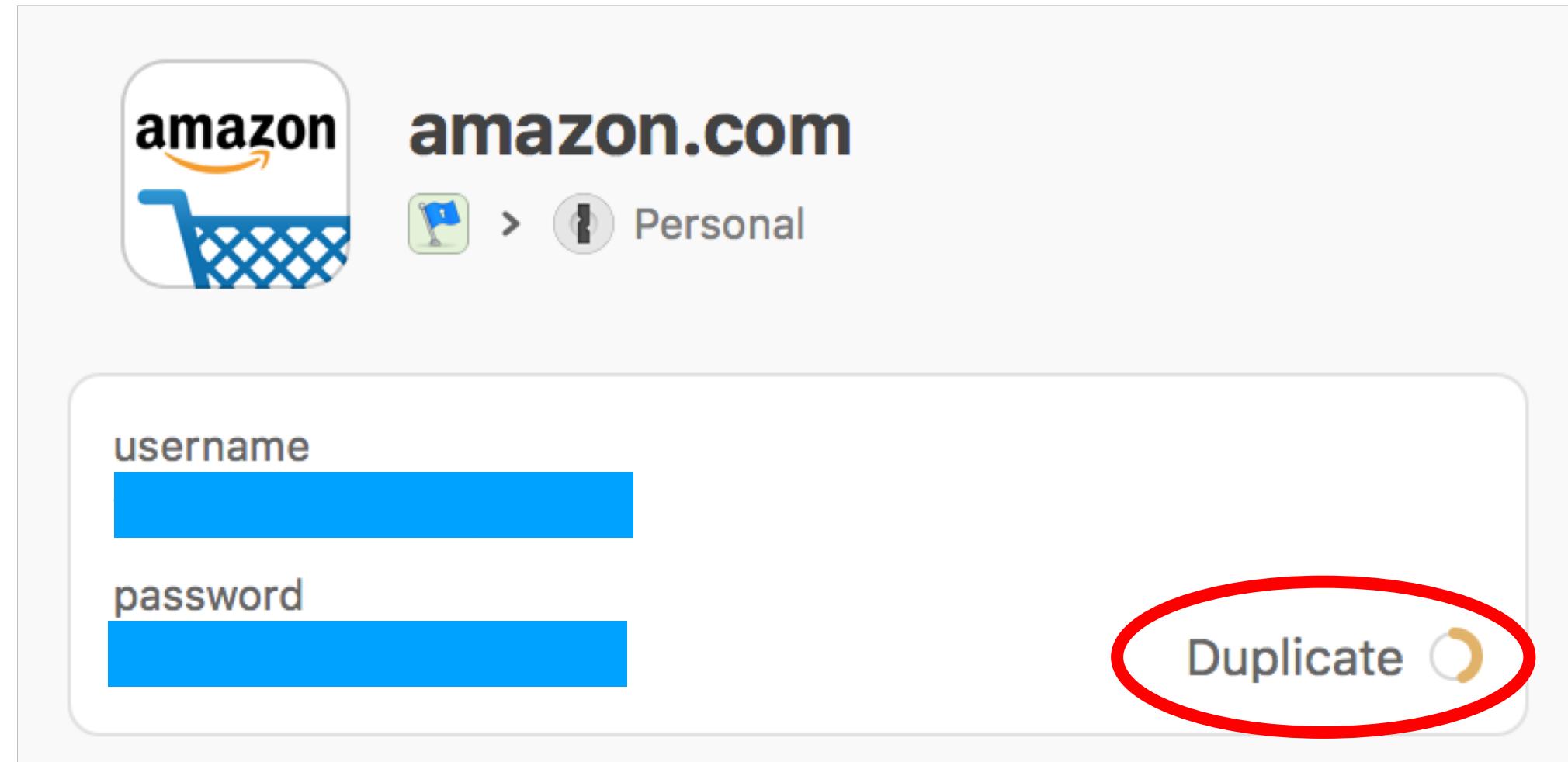
suggest unique passwords for other accounts



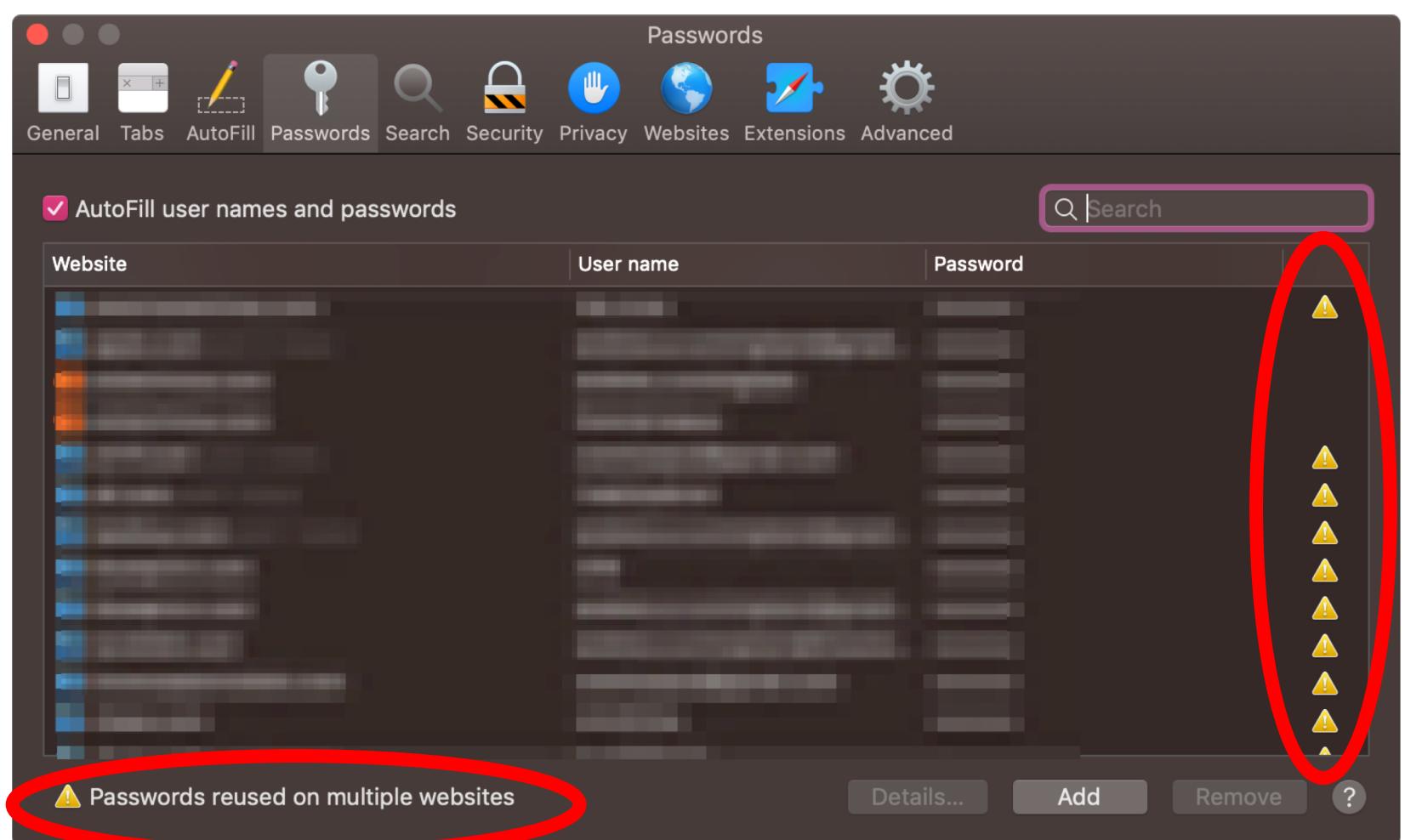
# conclusion

1. formative, systematic study of password-reuse notifications
2. developed best practices
3. future work should study novel notifications





1Password



macOS Mojave, Safari 12

All items	45
Favorites	12
Offline Changes	1
WATCHTOWER	
Compromised Logins	
Vulnerable Passwords	
Reused Passwords	2
Weak Passwords	1
Unsecured Websites	9
Inactive 2FA	4
Expiring	2

# 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

The screenshot shows an email inbox interface with a message from 'AcmeCo'. The message subject is 'Please create a new password'. The body of the email informs the recipient that their account may have been compromised due to a data breach at a different service. It advises creating a new password and provides links to the AcmeCo website and mobile app for password recovery. It also recommends enabling Two-Factor Authentication and changing other passwords. The message concludes with thanks from the AcmeCo Team.

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.

# Designing Password-Reuse Notifications

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



# extra slides

# representative notifications

The image displays three distinct notifications side-by-side:

- Gmail Inbox:** A red banner at the top of a browser window (https://mail.google.com/mail/#inbox) reads "Warning: Google prevented a suspicious attempt to sign in to your account using your password." It includes a "Review activity now" button.
- Instagram Profile (jane\_doe):** A modal window titled "Keep Your Account Secure" informs the user that their Instagram password is the same as one stolen from another site. It urges them to change their password and provides a "Change Password" button.
- Google Accounts Email:** A red header says "Someone has your password". The message body informs the user that someone used their password to try to sign in from Victoria Falls, Zimbabwe. It includes "Details", a timestamp (Sunday, October 30, 2016 9:38 PM), and a "REVIEW YOUR DEVICES NOW" button. The message concludes with "Best, The Google Accounts team".

# 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](http://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](tel:1-866-579-7172).

–The Netflix 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**

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

# “password-reuse notifications”

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

Not My Fault!



# 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

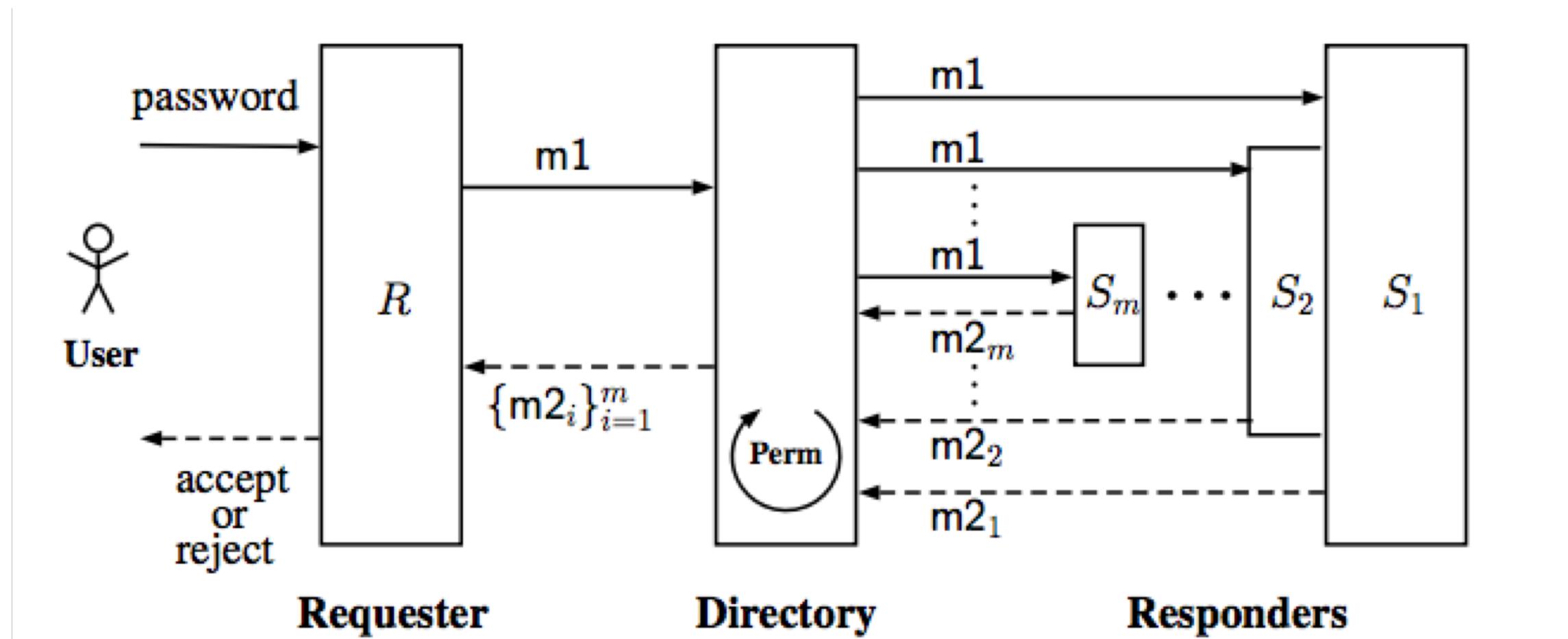
# How to End Password Reuse on the Web

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

The screenshot shows an email interface with a dark header bar containing three colored dots (red, yellow, green) and a 'Compose' button. Below the header is a toolbar with icons for reply, forward, and delete. The main area shows a message from 'AcmeCo' with the subject 'Please create a new password'. The message body starts with 'Dear Jo,' and discusses a potential security incident where login information may have been compromised. It includes a redacted section of text and ends with a call to action to create a new password. At the bottom, there's a section for security recommendations and links to more information.

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.

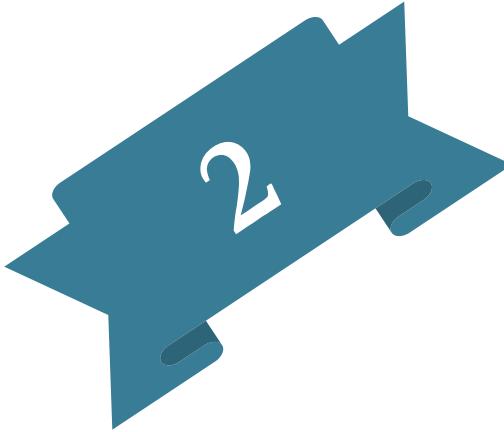
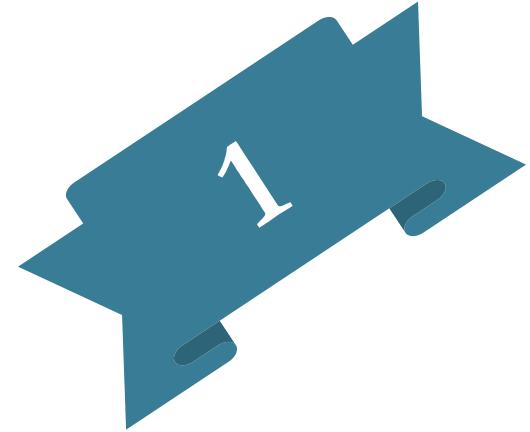
If you would like to learn more, please visit <https://acmeco.com/security>. If you have any questions or need any further assistance, please visit the Help Center at <https://acmeco.com/help>.

Thanks,  
The AcmeCo Team

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

<b>Delivery Medium</b>	
<i>model</i>	Delivered by email
<i>inApp</i>	Mobile in-app
<i>mobile</i>	Mobile push notification and in-app
<b>Incident</b>	
<i>model</i>	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.
<i>usBreach</i>	This incident was likely a data breach of one of our services.
<i>vagueCause</i>	—
<b>Account Activity</b>	
<i>model</i>	While we have not detected any suspicious activity on your AcmeCo account, ...as a precaution.
<i>suspicious</i>	Because we have detected suspicious activity on your AcmeCo account, ...
<i>omitActivity</i>	—
<b>Remediation</b>	
<i>model</i>	... you must create a new password ...
<i>recommend</i>	... we recommend that you create a new password.
<b>Other Accounts</b>	
<i>model</i>	Change all similar passwords on other accounts.
<i>noOthers</i>	—
<b>Extra Actions</b>	
<i>model</i>	To further improve your online security, we recommend:
<i>noExtras</i>	<ul style="list-style-type: none"><li>• Enabling AcmeCo's Two-Factor Authentication.</li><li>• Using a password manager.</li></ul> —

# covariates



- CS literacy      ???
  - Gender
  - ...