

“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 

 **reddit**

 **淘宝网**
Taobao.com

 **Baidu** 百度

 **WELLS FARGO**

 **1&1**

 **Dropbox**

 **facebook**

 **airbnb**



 **twitter** 

 **Adobe**

 **eBay**

 **YouTube**

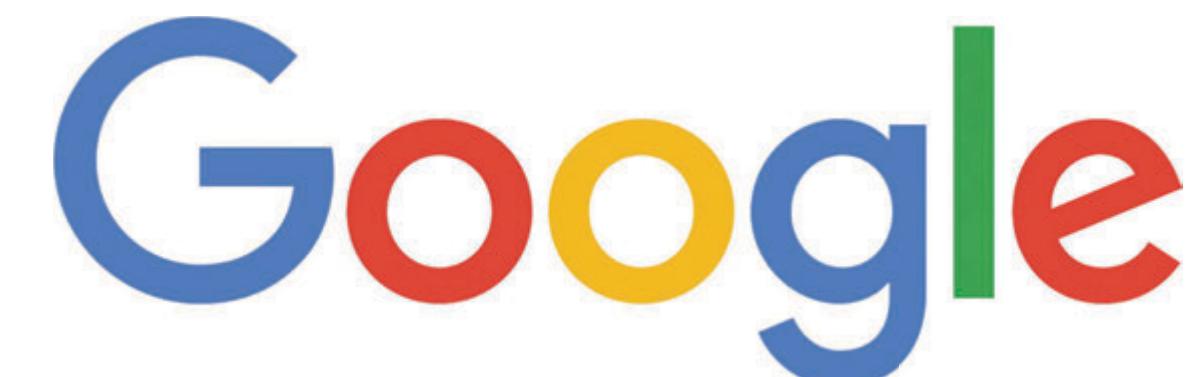


Microsoft



slack

SONY

 **Google**

“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 items sorted by title, starting with 'A'. The 'Apple ID (iCloud)' item is selected and shown in detail on the right. The detailed view includes:

- Apple ID (iCloud)**: Personal account for wendy.c.appleseed@gmail.com.
- username**: wendy.c.appleseed@gmail.com
- password**: (redacted)
- Apple ID**: <https://appleid.apple.com/#!&page=signin>
- iCloud**: <https://www.icloud.com>
- SECURITY**
 - best friend: (redacted)
 - parents city: (redacted)
 - mother's maiden: (redacted)

people reuse passwords

Booking.com

R0cky!14



reddit

R0cky!17

淘宝网
Taobao.com

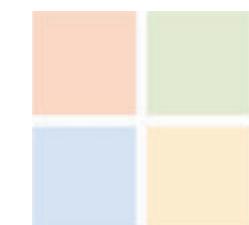
American Airlines

facebook

R0cky!17



123456



Microsoft

Rocky!16

ebay

YouTube

ROckyStar

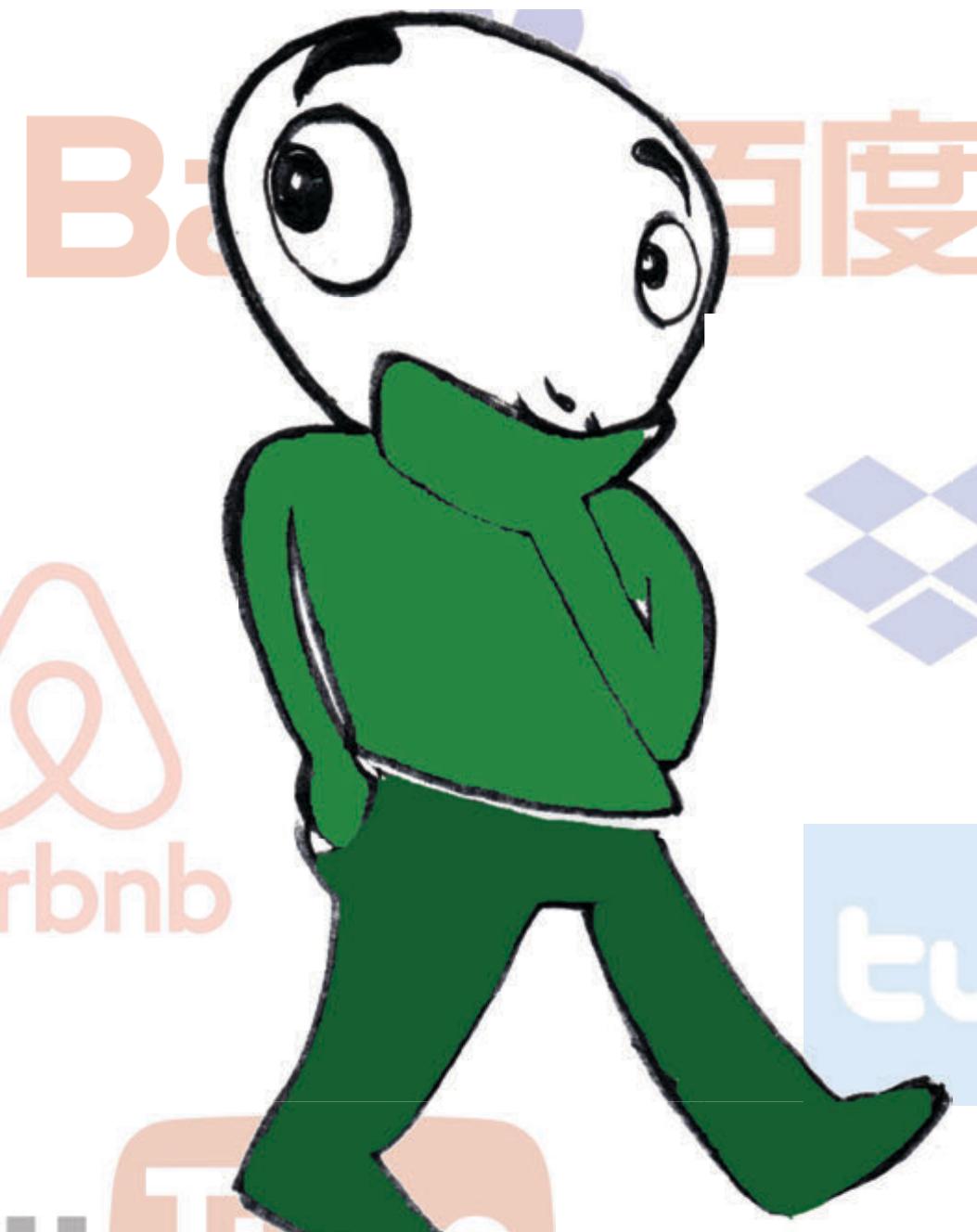
SONY

slack



Google

ROcky!17





Memory-Hard Hash Function



Rate-Limiting Guessing



I'm not a robot

reCAPTCHA
Privacy - Terms

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

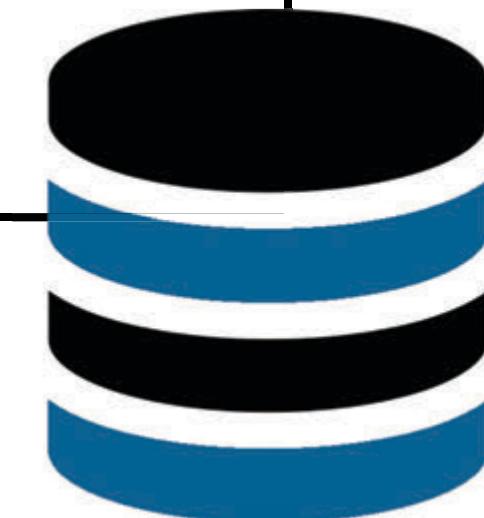


LinkedIn





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
...	...



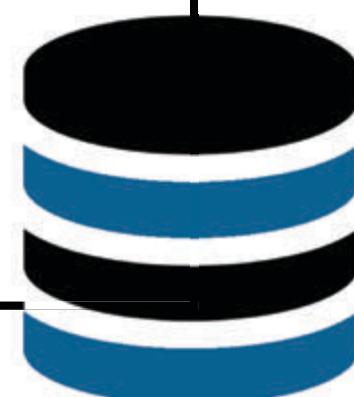
crack all the things!



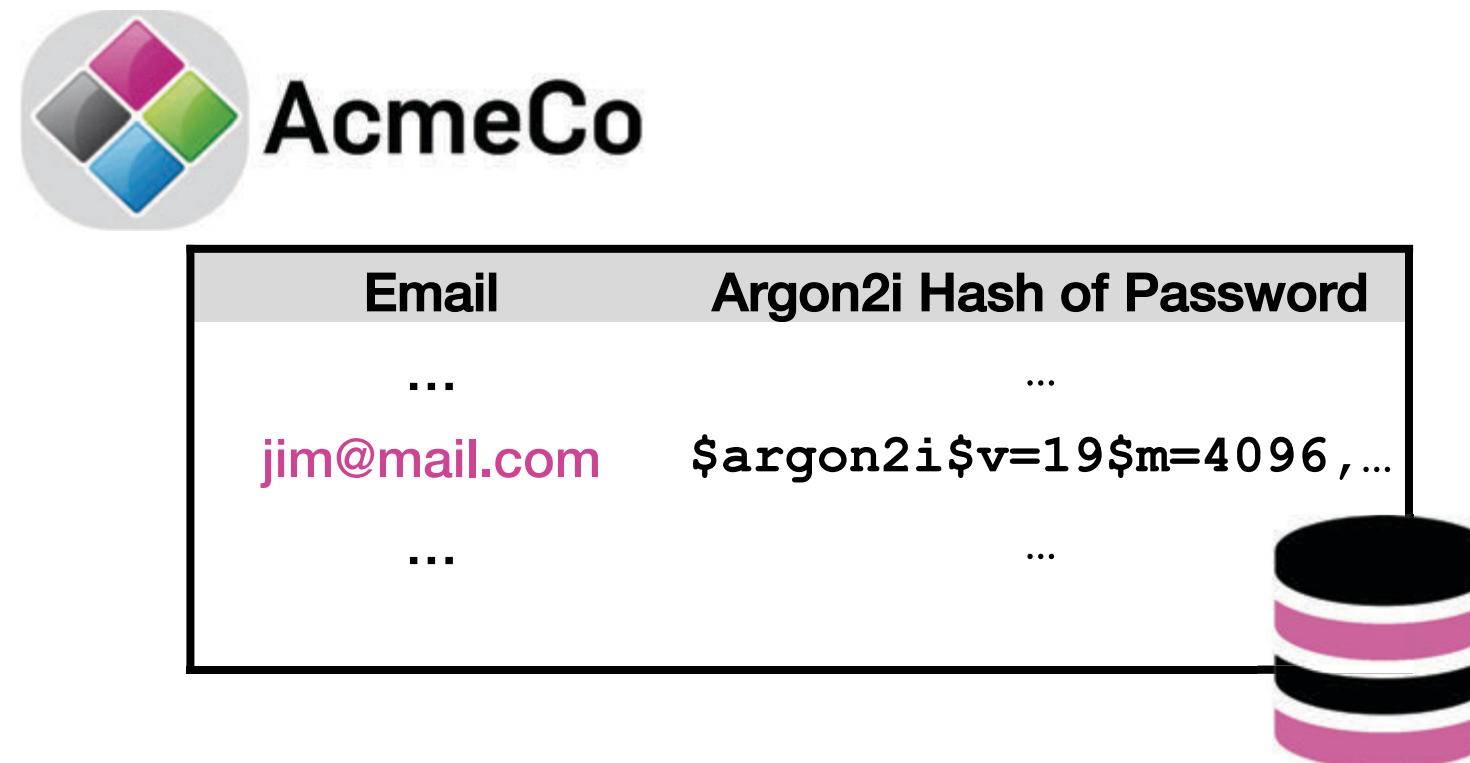
```
Bash
$> hashcat -m 100 -a0 $TARGET $DICT
123456
Password
R0cky!17
Football!17
CanadaRocks!
```



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
...	...



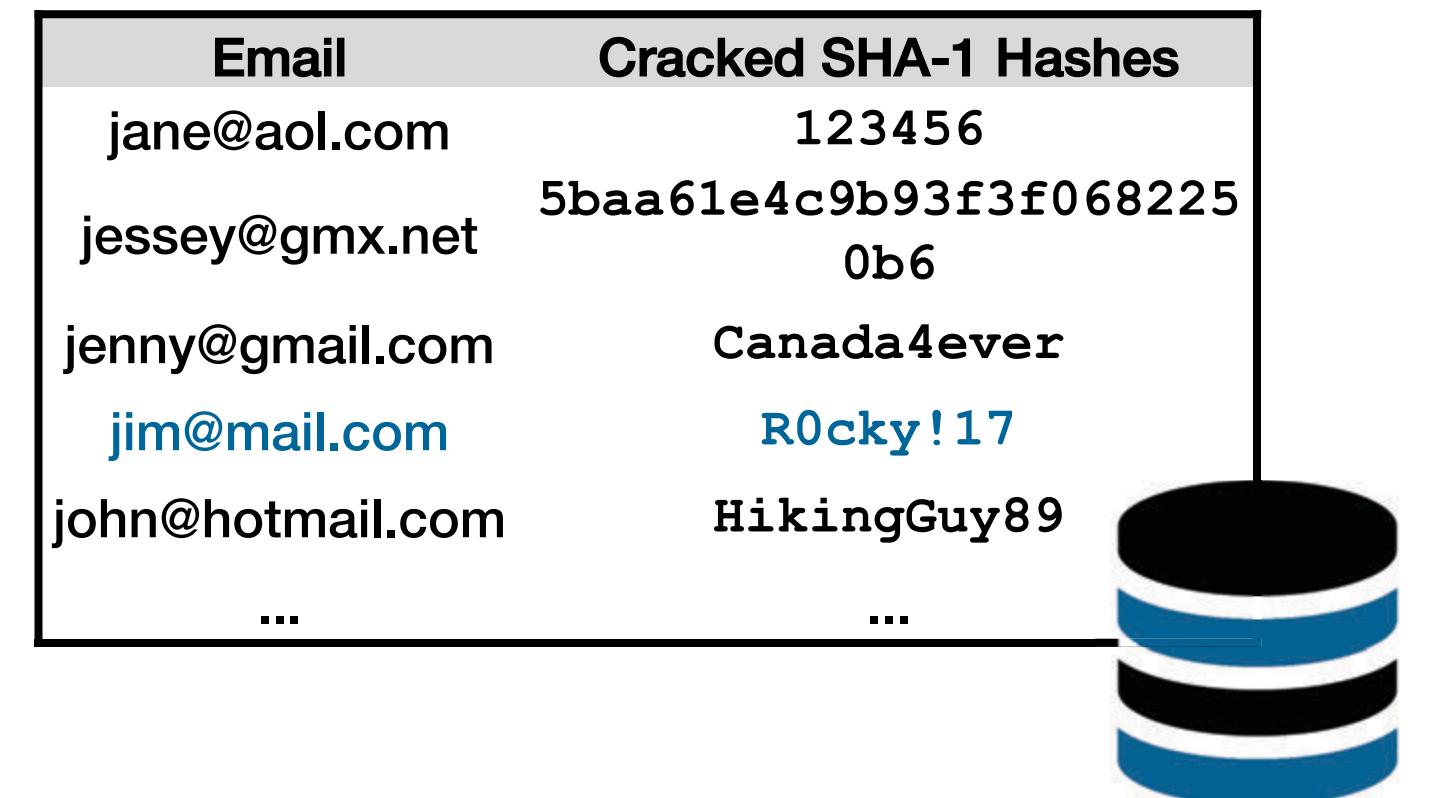
dead on arrival



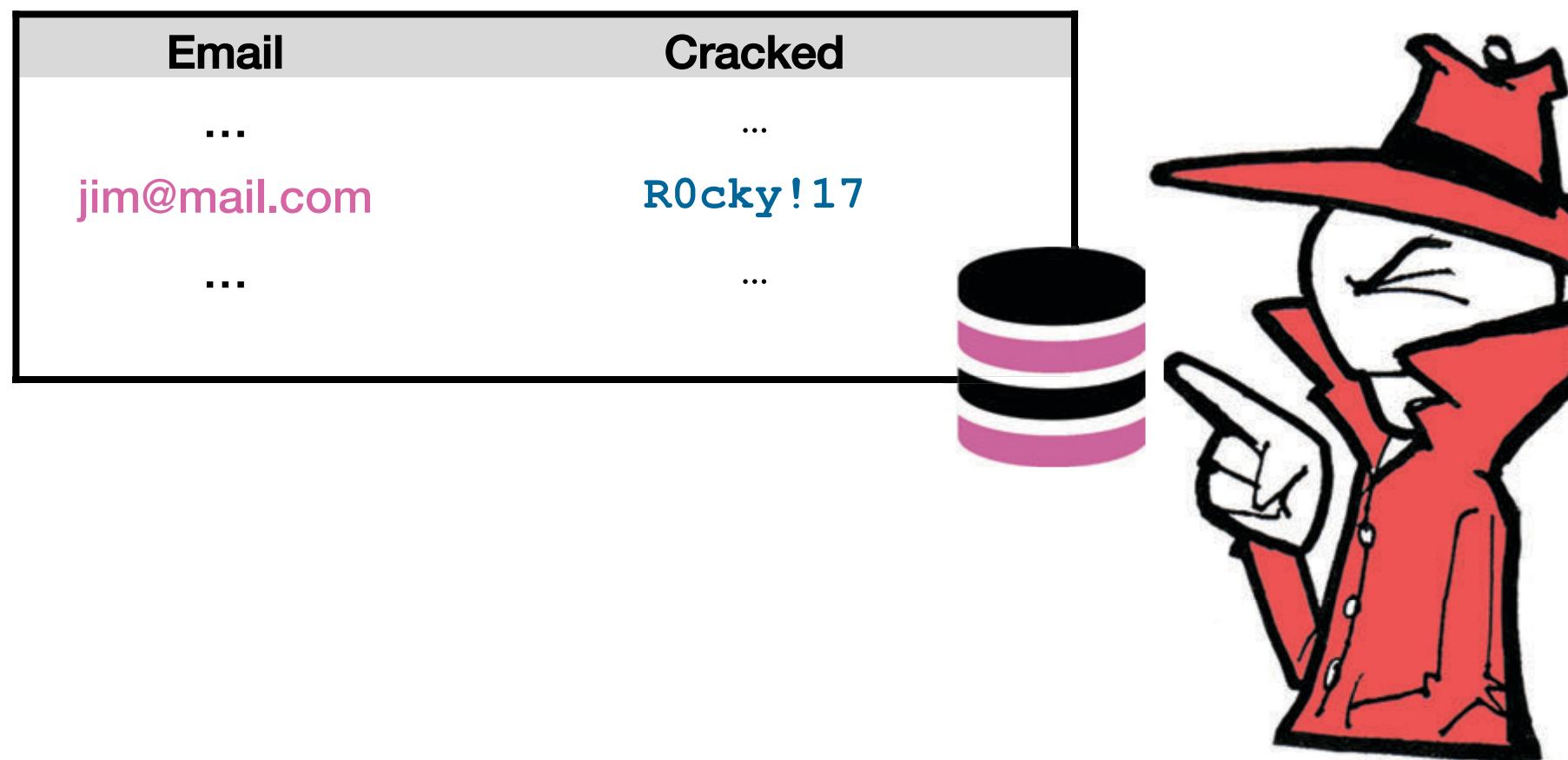
dead on arrival



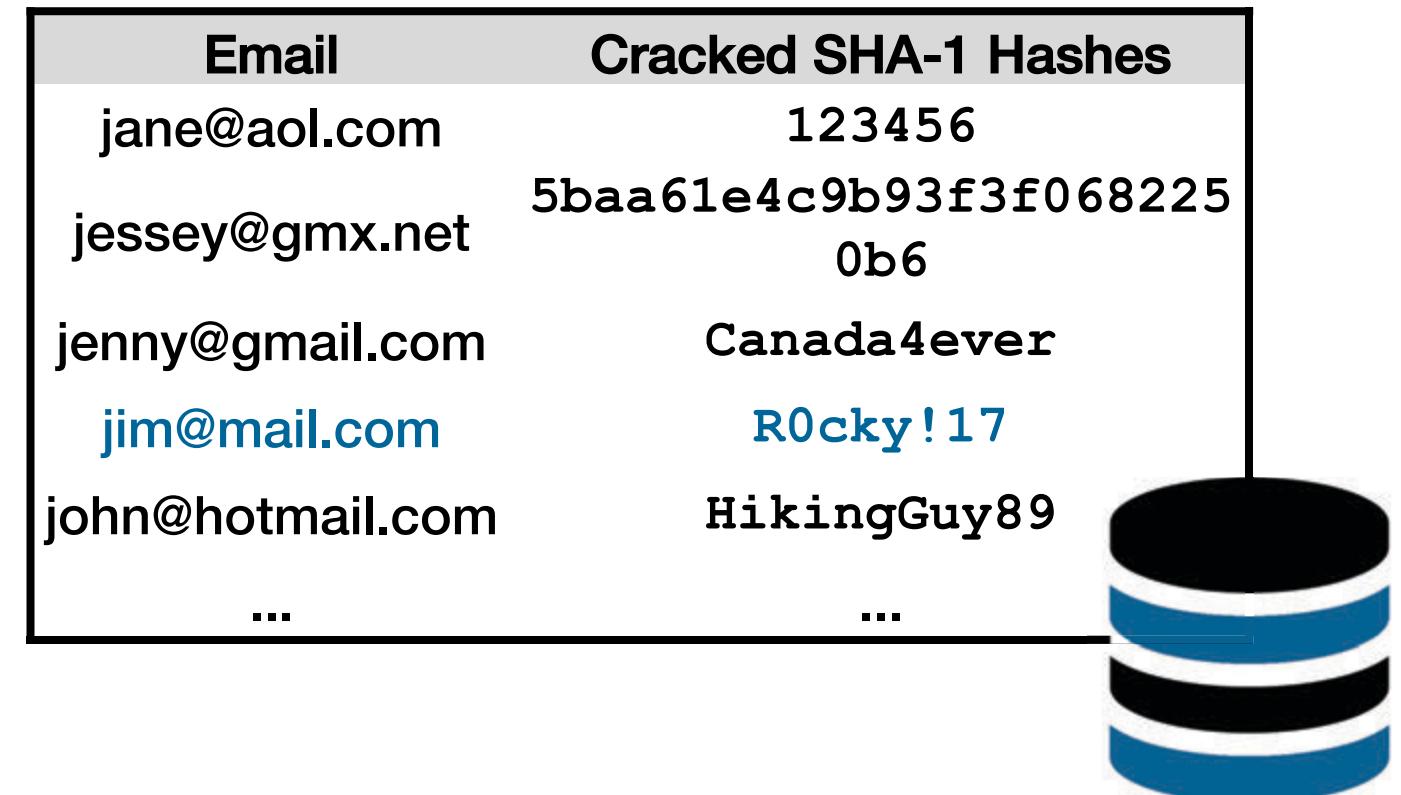
LinkedIn



dead on arrival



**1 guess is
enough!**



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

'--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

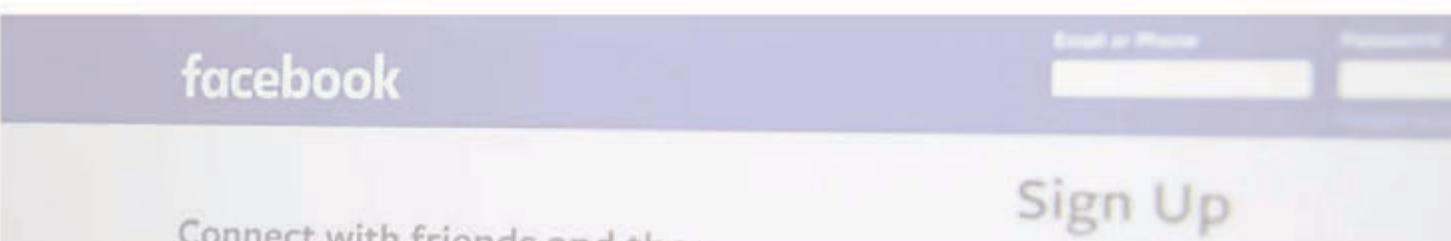
87,820,647

paste accounts

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-
BICCIERI
STAFF WRITER



black market monitoring

The screenshot shows a web browser window for a dark web marketplace. The URL in the address bar is `trdealmgm4uvn42g.onion/listing/3600`. The page header includes a welcome message "Welcome back, [REDACTED]", notification counts (0 notifications, 0 messages, 0 items), a balance of "BTC 0.0000", and navigation links for "Home", "My RealDeal", "Support", and "Logout". A search bar at the top right contains the placeholder "I want to order ...".

The main content area displays a listing for "LinkedIn 167M" by user "peace_of_mind" (100.0%, Level 1 (14)). The listing price is "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 "Qty: 0" and a large red "Buy It Now" button. Below the listing are details: "Escrow" (Yes, escrow by RealDeal is available), "Class" (Digital), and "Ships From" (Worldwide). There are also "Favorite" and "Question" buttons.

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?

Freelancer

Dear [REDACTED],
We are writing to let you know that we have reset your Freelancer.com password because we have detected login credentials that match yours in a publicly accessible database related to a compromise of a third party website.

The compromise of your username and password did not occur through any Freelancer.com operated web property. You can discover the source leak(s) of your credentials using the following (free) service: <http://haveibeenpwned.com>

Currently, the "mega leak" of compromised accounts from third-party websites have over 3.8 billion entries and include leaks from websites including LinkedIn, Elance, Dropbox and Adobe.

As a precautionary security measure, we have reset your Freelancer password, and require you to create a new one, please be sure to use a new unique password.

[Click Here to Create Your New Password](#)

If you have any questions about resetting your password please contact the Freelancer Support Team at support@freelancer.com.

Regards,
Freelancer Security Team

Houzz

Important information regarding your Houzz account

Houzz <noreply@houzz.com> To me 10:13 PM (12 hours ago)

This message has been deleted. [Restore message](#)

Spotify

Please update your Spotify password.

Hi AvatarWalt,

Our security team noticed that you from another service that was re

As a precaution, and to protect you update your password to access [forgotPassword](#).

As a reminder, it is a best practice if you share them across service

Thanks,
The Houzz Team

RESET PASSWORD

If this button did not work, please click here for how to reset your password manually. www.spotify.com/password-reset/

To ensure the security of your account, we suggest changing the password with which you use the same one.

Spotify

Please Confirm Your Identity

Hi James

To protect your Spotify account, we've reset your password. This is because we believe it may have been compromised during a leak on another service with which you use the same password.

Don't worry! This is purely a preventative security measure. Nobody has accessed your Spotify account, and your data is secure.

To create a new password for you can log back into Spotify, simply click the big green button below.

Gmail

Someone has your password

Blase Ur <blaseur@gmail.com>

Related Google+ Page

Google <no-reply@accounts.google.com> To: blaseur@gmail.com Sun, Oct 30, 2016 at 2:38 PM

Reset Your Password

This action is being taken proactively and at this time there is no evidence to indicate that your account or data have been compromised. Your backups are safe and your regular backup schedule will continue.

What Happened

As part of our ongoing security monitoring, we recently became aware of unauthorized attempts to access a number of Carbonite accounts. This activity appears to be the result of a third party attacker using compromised email addresses and passwords obtained from other compromised accounts. We are investigating this activity and taking steps to reduce the risk to our users by updating the security measures we have in place to protect the data stored in our systems.

What Information Was Involved

As part of our ongoing security monitoring, we recently became aware of unauthorized attempts to access a number of Carbonite accounts. This activity appears to be the result of a third party attacker using compromised email addresses and passwords obtained from other compromised accounts. We are investigating this activity and taking steps to reduce the risk to our users by updating the security measures we have in place to protect the data stored in our systems.

What Are Doing

To ensure the protection of our customers and the safety of their data, we are requiring all Carbonite customers to reset their login information. Our Customer Care team is standing by to assist anyone who needs additional help. This activity is in no way affects existing or scheduled backups. Please rest being safely backed up.

In addition to our existing monitoring practices, we will be rolling out additional security measures to protect your account, including increased security review and two-factor authentication (which we strongly encourage you to use).

What You Can Do

Use the above to reset your password. We highly recommend using "long" unique passwords for Carbonite and all online accounts. Learn more about strong passwords at www.carbonite.com/safety. If you use the same or similar passwords or other online services, we recommend that you set new passwords on those accounts as well.

For more information please contact Customer Care at <https://support.carbonite.com>.

Spotify

Please Confirm Your Identity

Hi in attempt to your account.

Hi maximilian.golla@gmail.com>

in attempt to your account.

Wed, Sep 6, 2017 at 3:22 PM

Please Confirm Your Identity

Google

Someone has your password

Hi Blase,

Someone just used your password to try to sign in to your Google Account blaseur@gmail.com.

Details:

Sunday, October 30, 2016 9:38 PM (Central Africa Time)
Victoria Falls, Zimbabwe*

Google stopped this sign-in attempt, but you should review your recently used devices:

Microsoft account

From: Microsoft account team Date: Friday, April 17, 2015 at 6:26 AM Subject: Microsoft account unusual sign-in activity

Best,
The Google Account

*The location is app
This email can't be read
Center.

Microsoft account

Unusual sign-in activity

We detected something unusual about a recent sign-in to the Microsoft account *****@comcast.net. To help keep you safe, we required an extra security challenge.

Sign-in details:
Country/region: United States
IP address: 55.5.555.55
Date: 4/17/2015 6:26 AM (EST)

If this was you, then you can safely ignore this email.

If you're not sure this was you, a malicious user might have your password. Please review your recent activity and we'll help you take corrective action.

Review recent activity

To opt out or change where you receive security notifications, [click here](#).

Thanks,
The Microsoft account team

Amazon

Hello,

At Amazon we take your security and privacy very seriously. As part of our routine monitoring, we discovered a list of email addresses and passwords posted online. While the list was not Amazon-related, we know that many customers reuse their passwords on multiple websites. Since we believe your email addresses and passwords were on the list, we have assigned a new password to your Amazon.com account out of an abundance of caution.

Insert your password when you return to the Amazon.com site. To reset your password, click "Your Account" page on Amazon.com. On the Sign In page, click the "Forgot your password?" link to reset your password. We'll send you an Assistance code. After you enter your email or mobile phone number, you will receive an email with instructions on how to reset your password.

Pinterest

Someone May Have

Recently, there was a security incident.

From: Pinterest Subject: We have detected suspicious activity on your Pinterest account

Reply to: no-reply@pinterest.com To: Ajay2

Hi, Ajay

We think someone may have logged into your Pinterest account without your permission. Please create a new password to secure your account.

LinkedIn

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

2615 posts 1073 followers 883 following

Instagram

More information:

Someone just logged into your Pinterest account from a new location in India. To protect your pins, we've put your account in read-only mode - no changes can be made to your pins or account settings until you secure it with a new password. After you create a new password, your account will be fully functional.

Thanks,

Netflix

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 "Sign in", and then click "Forgot your 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 <http://help.netflix.com/help> or call us at 1-866-579-7172.

Questions? Call 1-866-579-7172

This account email has been sent to you as part of your Netflix membership. To change your email preferences or any time, please visit the Communicate tab for your account. Please do not reply to this email if you do not recognize the email address. If you need help or would like to contact us, please visit our Help Center at help.netflix.com.

This message was mailed on: 09/09/2016 10:59:47 AM (US)
Using: 10.10.10.10
Our entire service and website is subject to our Terms of Use and Privacy Statement.
100 Wheeler Circle, Los Gatos, CA 95032, U.S.A.

Facebook

Your email address or profile URL*

Enter your email address or profile URL

Someone May Have

In order to keep your account safe, we will verify your email address. A link to reset your password will be emailed to all addresses associated with your account. To learn more, [visit our Help Center](#).

Request a password reset

LinkedIn

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

RUB

MARYLAND

SUPER



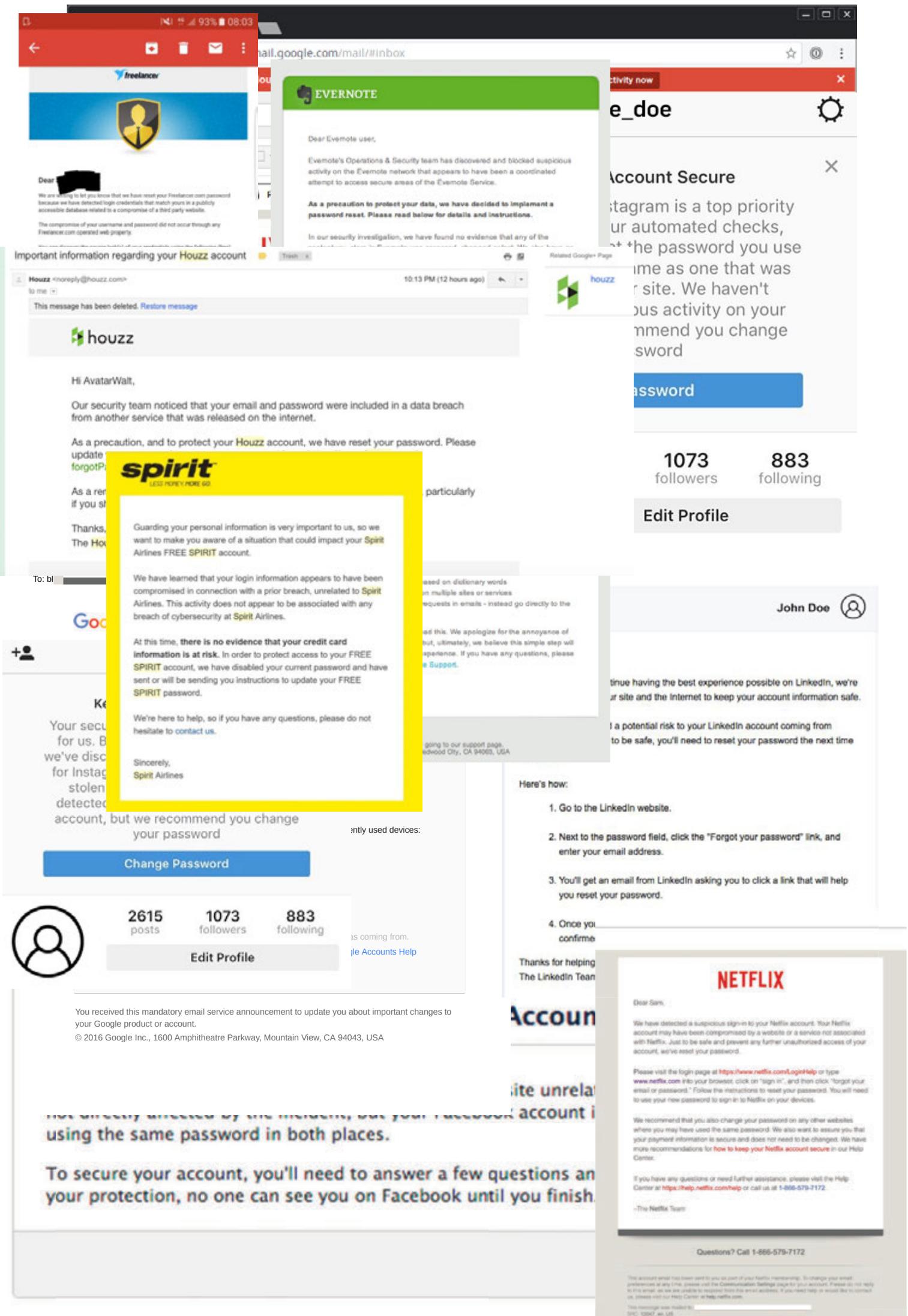
Keep your account secure

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

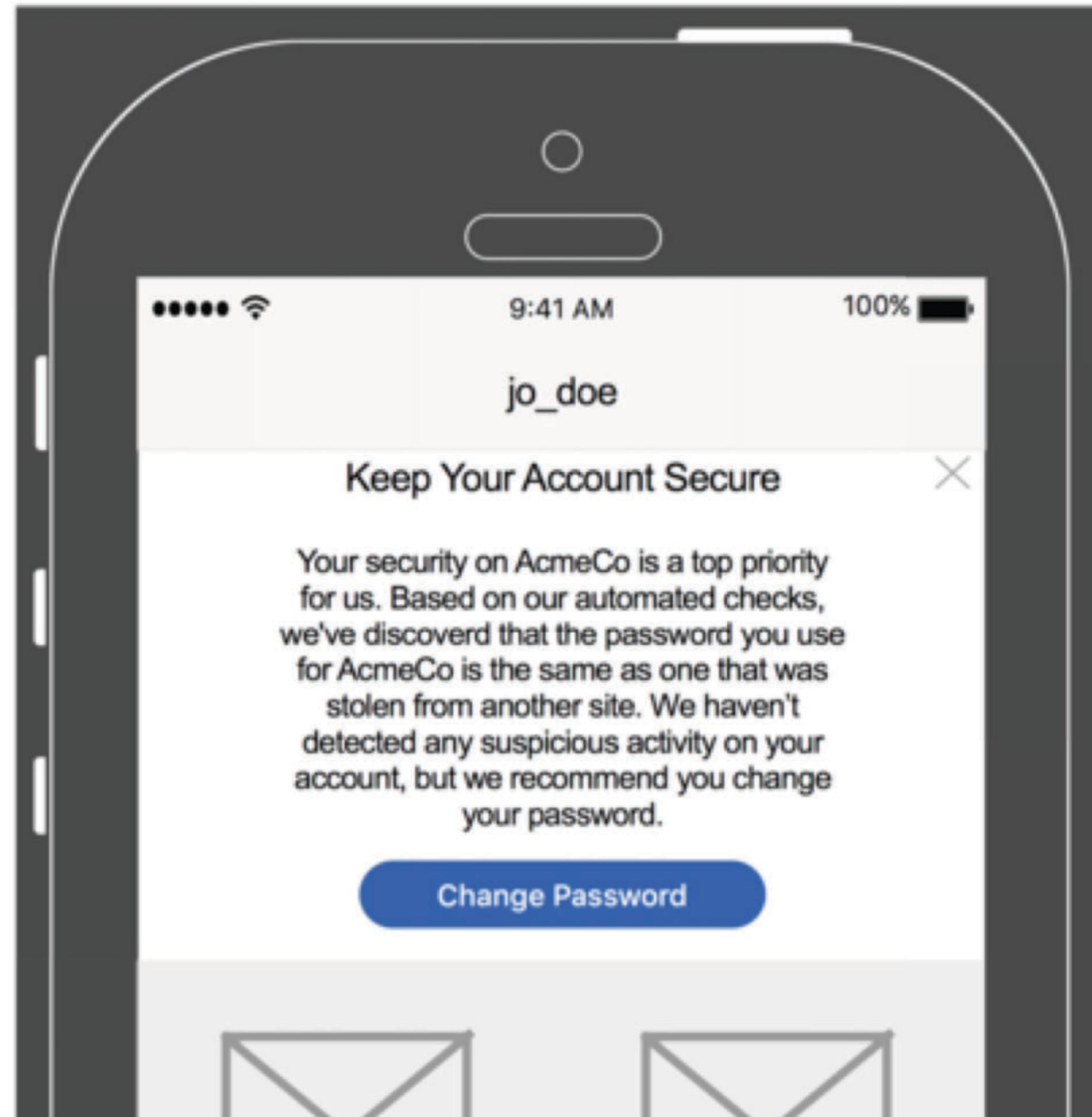
previously sent password-reuse notifications

STUDY 2

individual components of password-reuse notifications

Imagine you have an
important account with
AcmeCo...

AcmeCo notifications



questions asked

**notification
understanding**



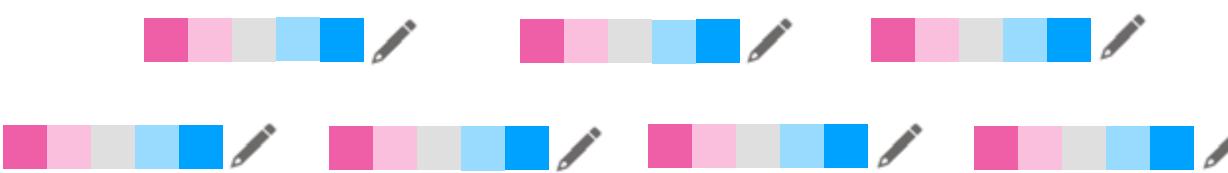
feelings



actions



perceptions



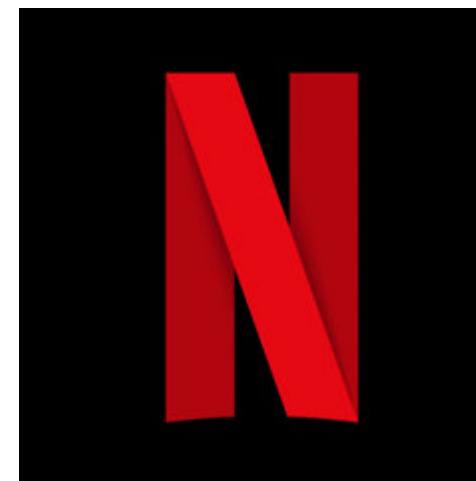
demographics

survey setup

180 respondents

- Amazon MTurk
- 15 mins
- Compensated \$2.50

6 conditions



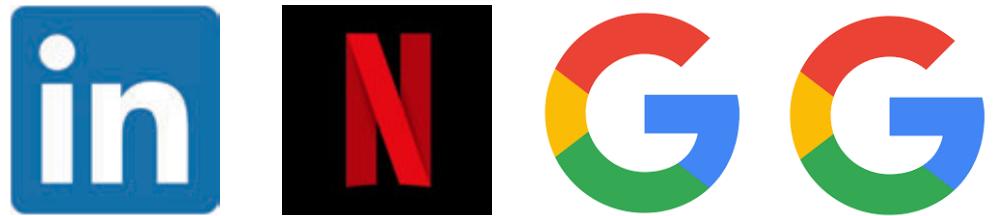
notifications were concerning and a priority



Why did you receive this notification?

60% hacked account

21% data breach



don't mention
password reuse



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](#)

*“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

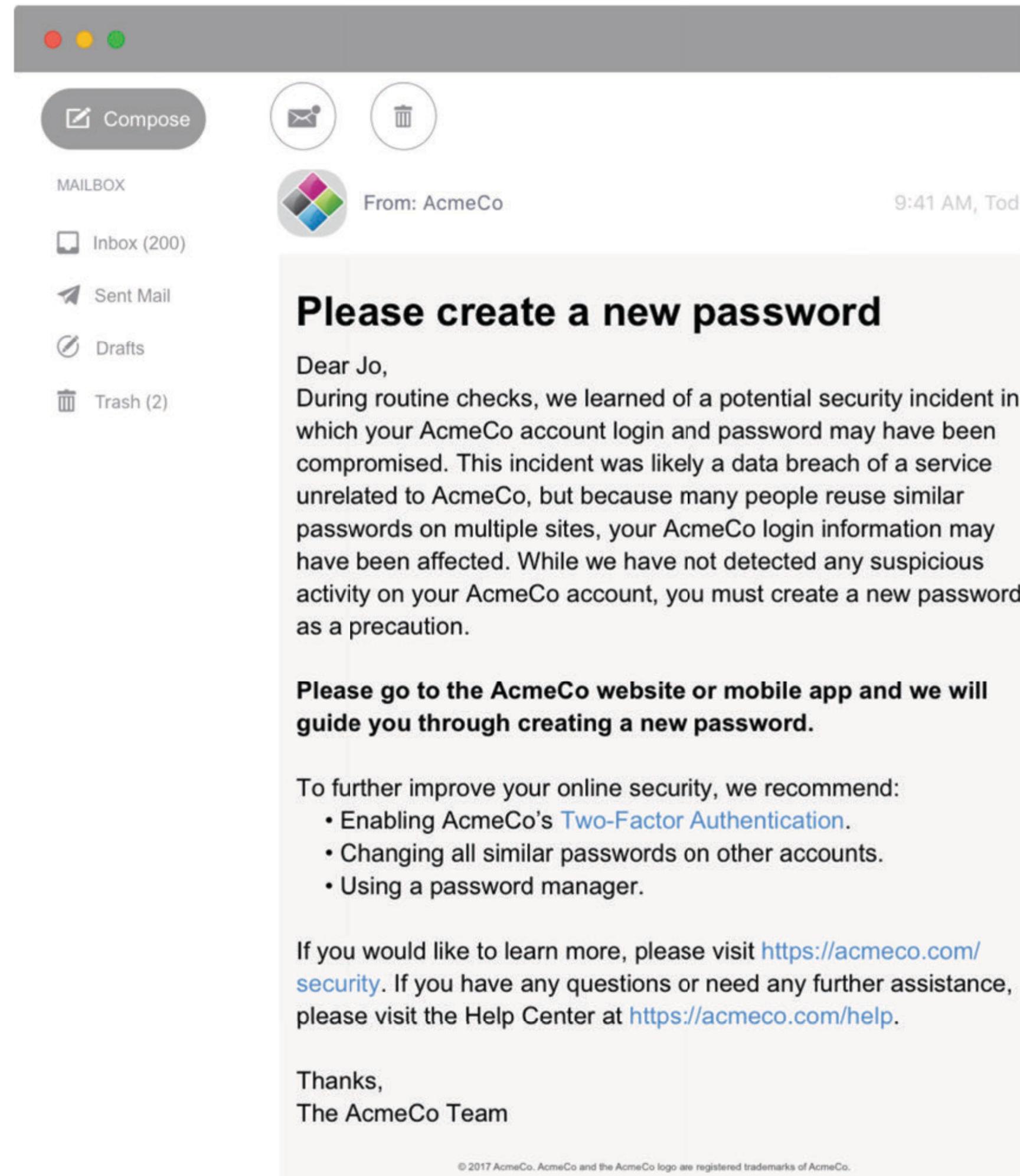
sufficient
background

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%

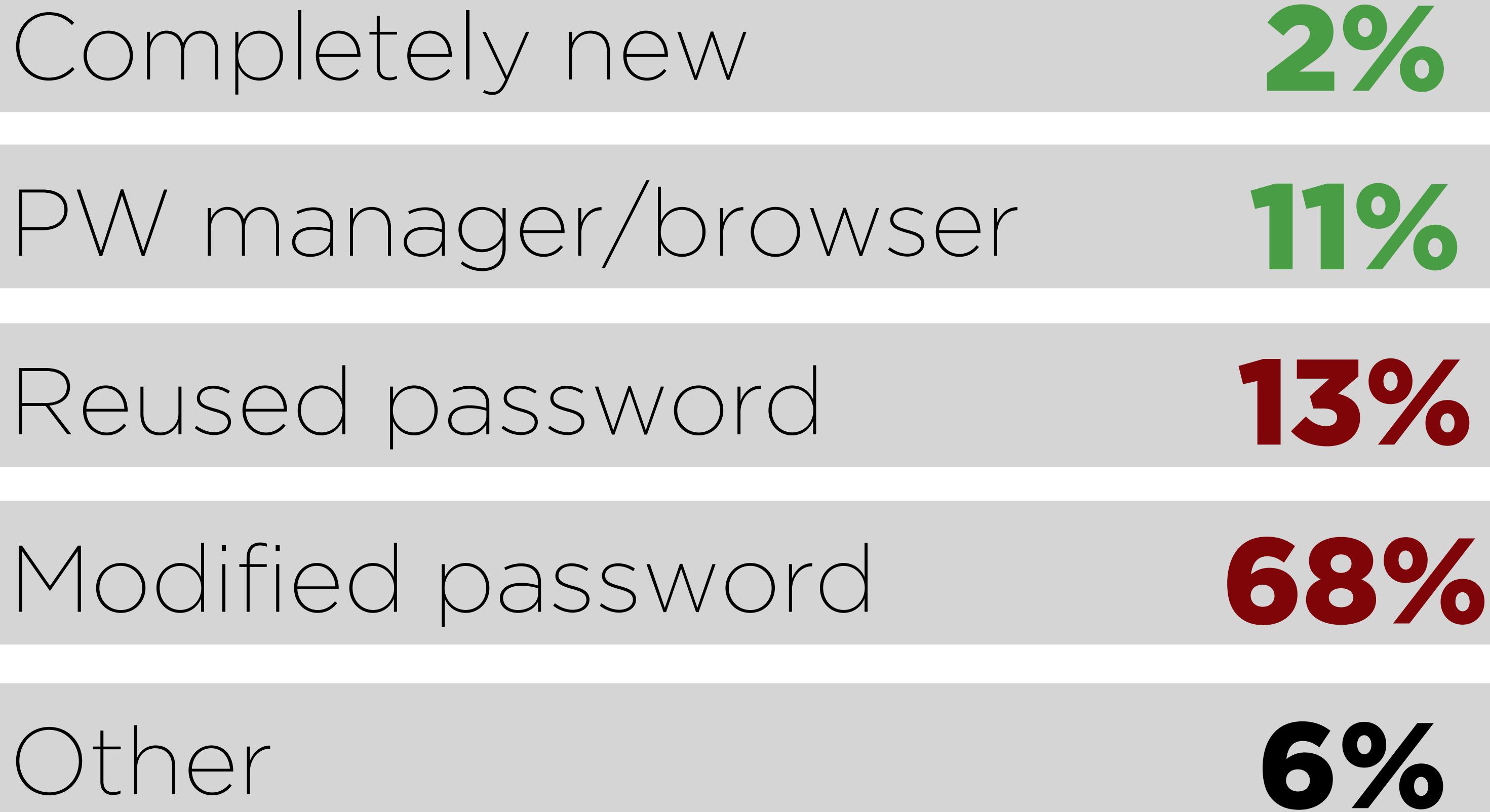
Change it

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

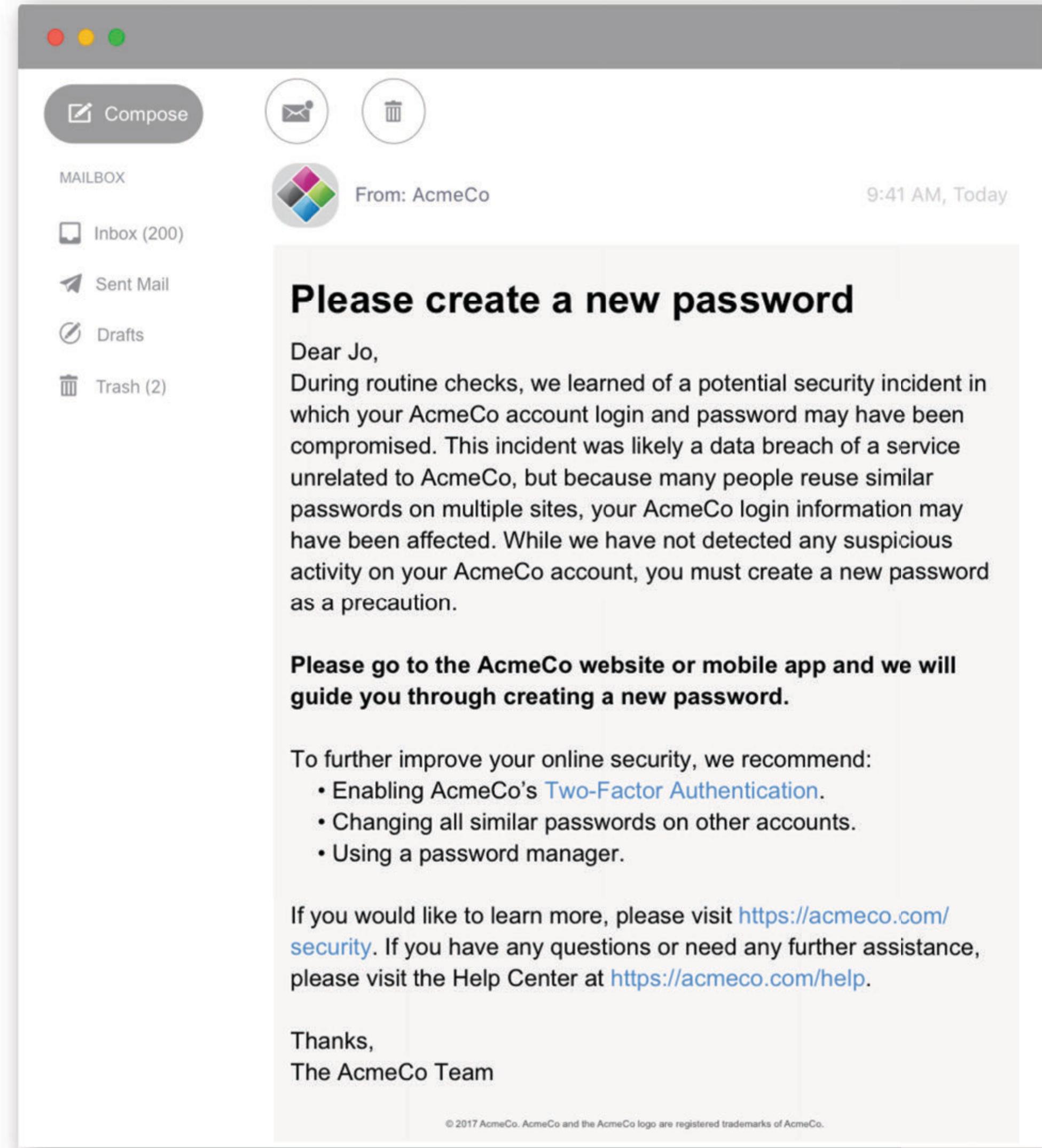
send via email + more immediate channel

name password reuse as root cause

force password reset

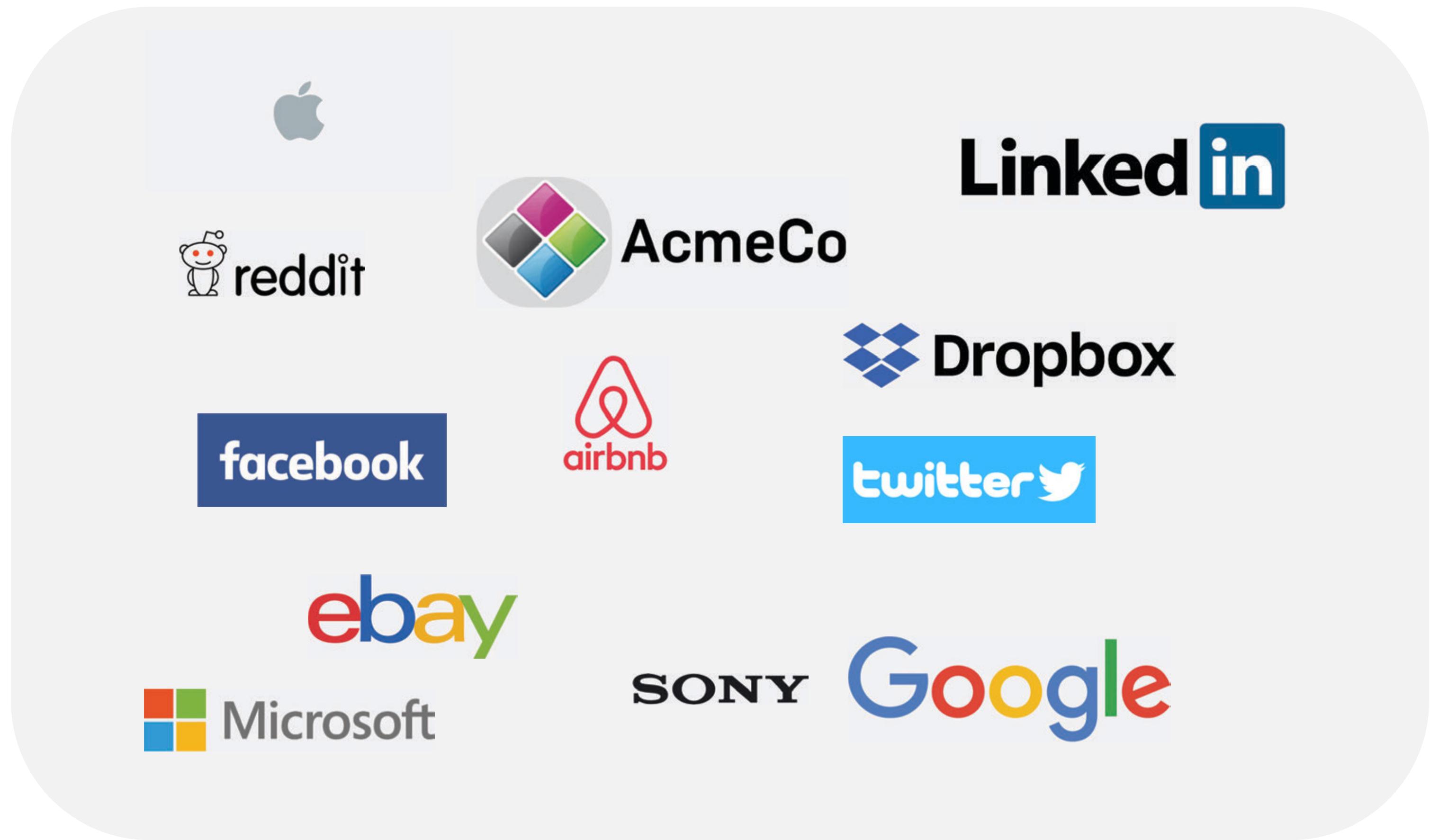
encourage 2FA and password managers

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



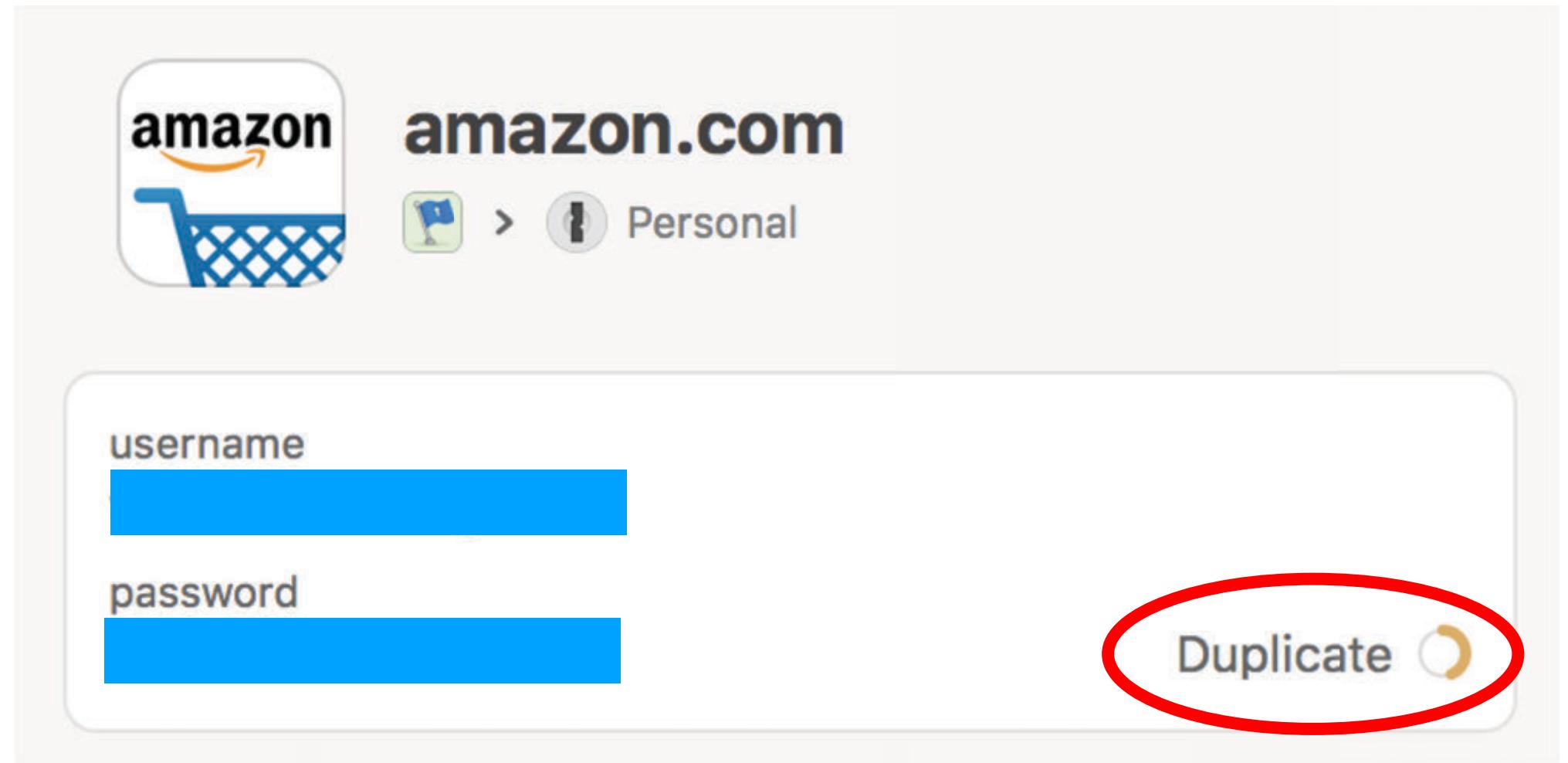
LastPass...!

True Key

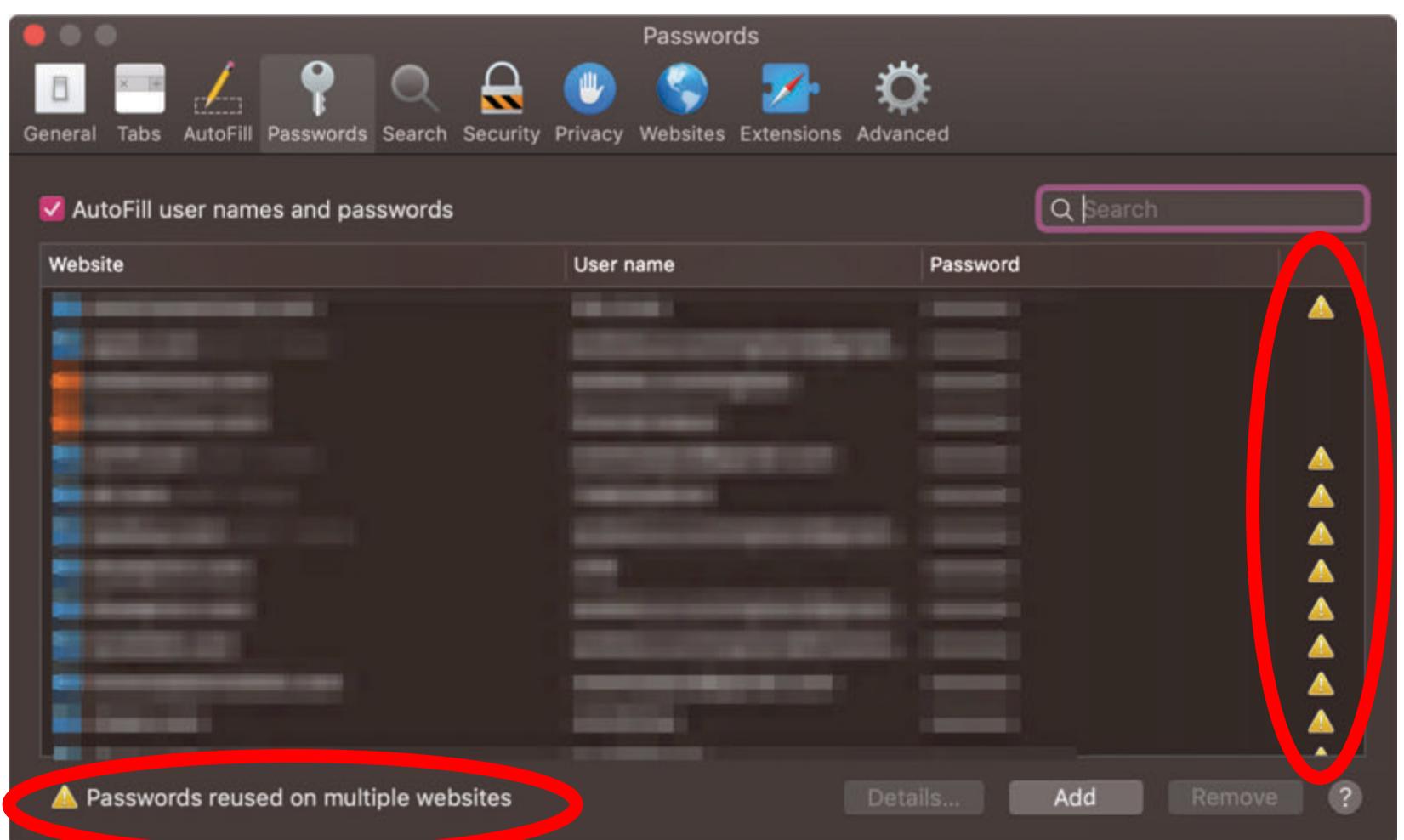
1Password

dashlane

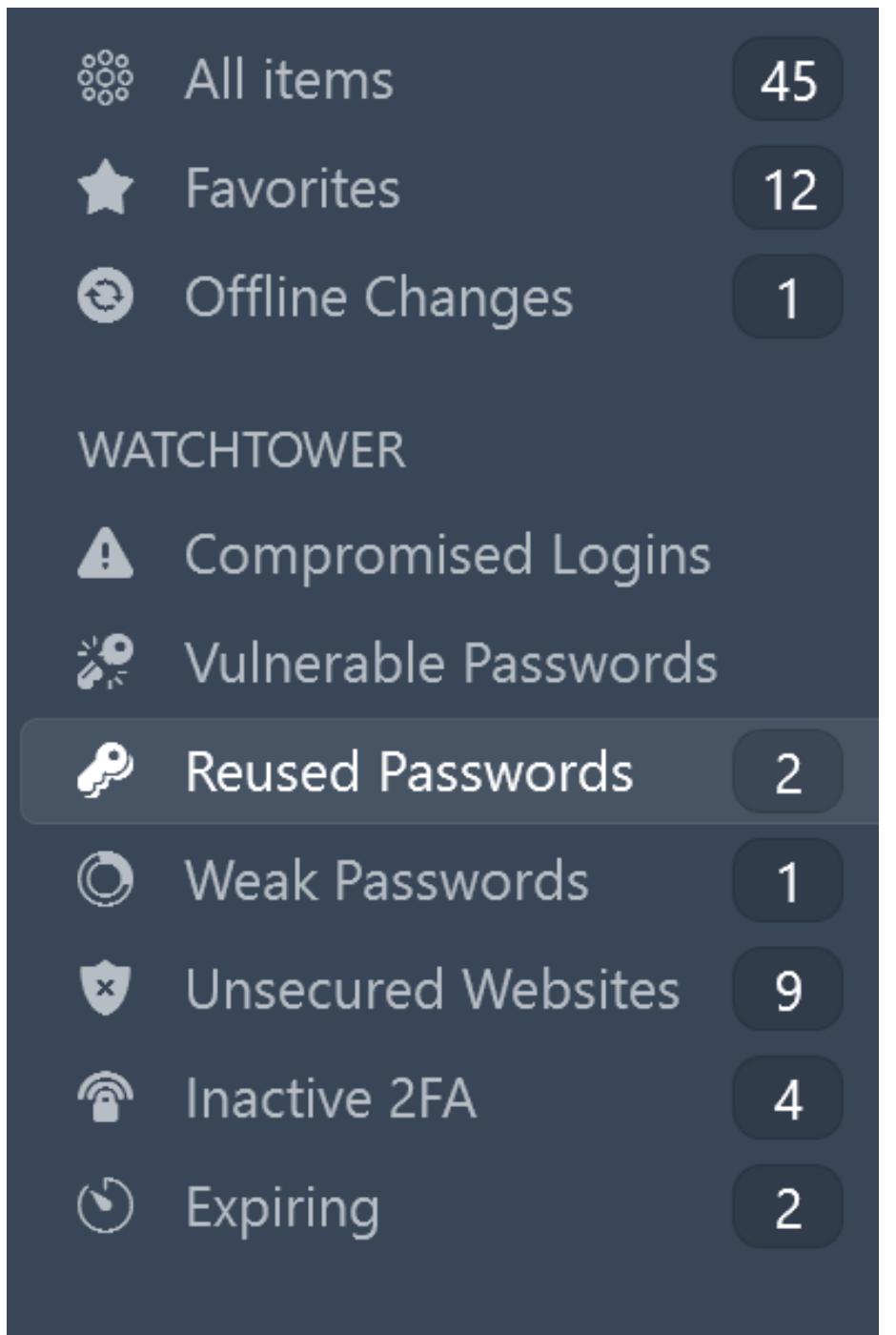




1Password

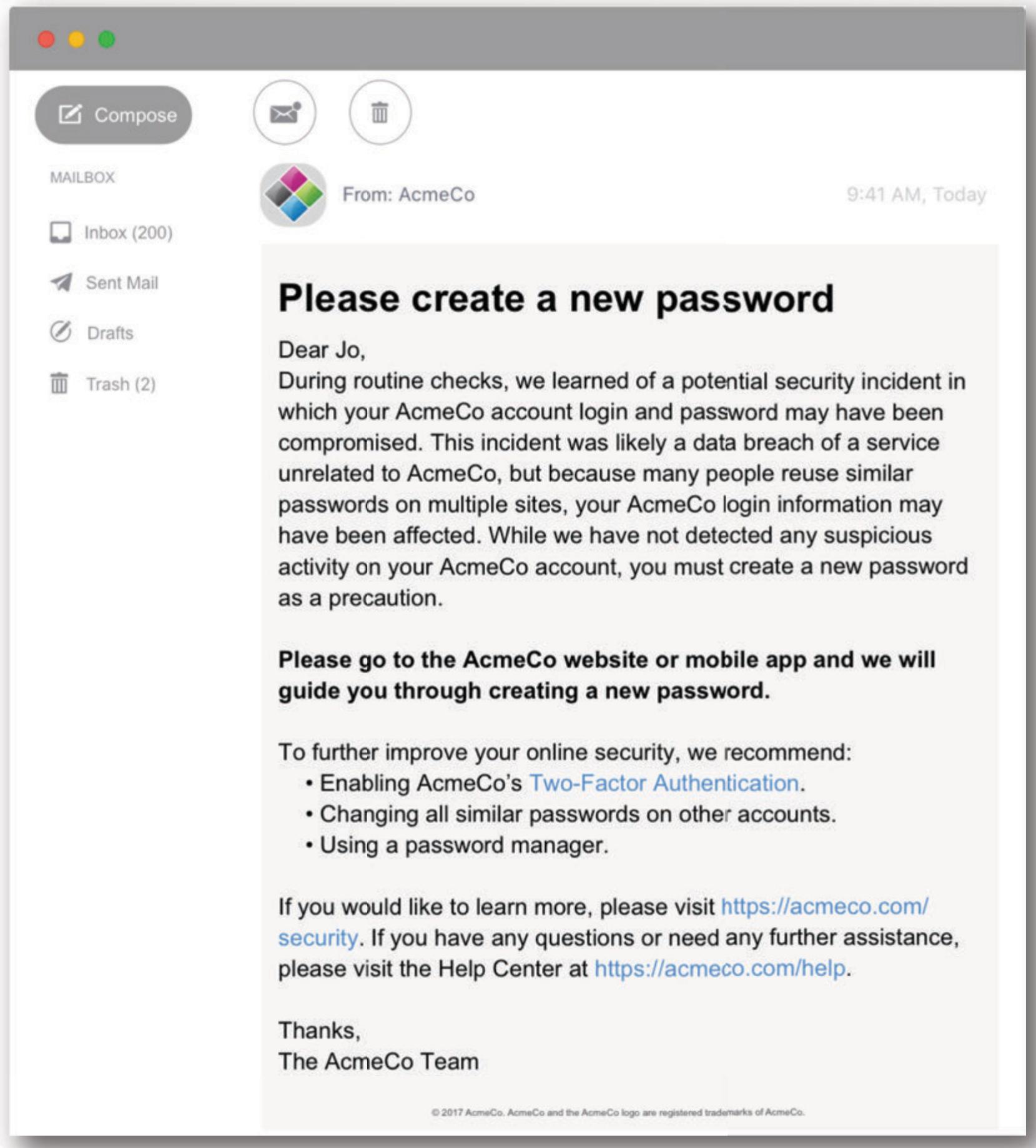


macOS Mojave, Safari 12



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

