“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

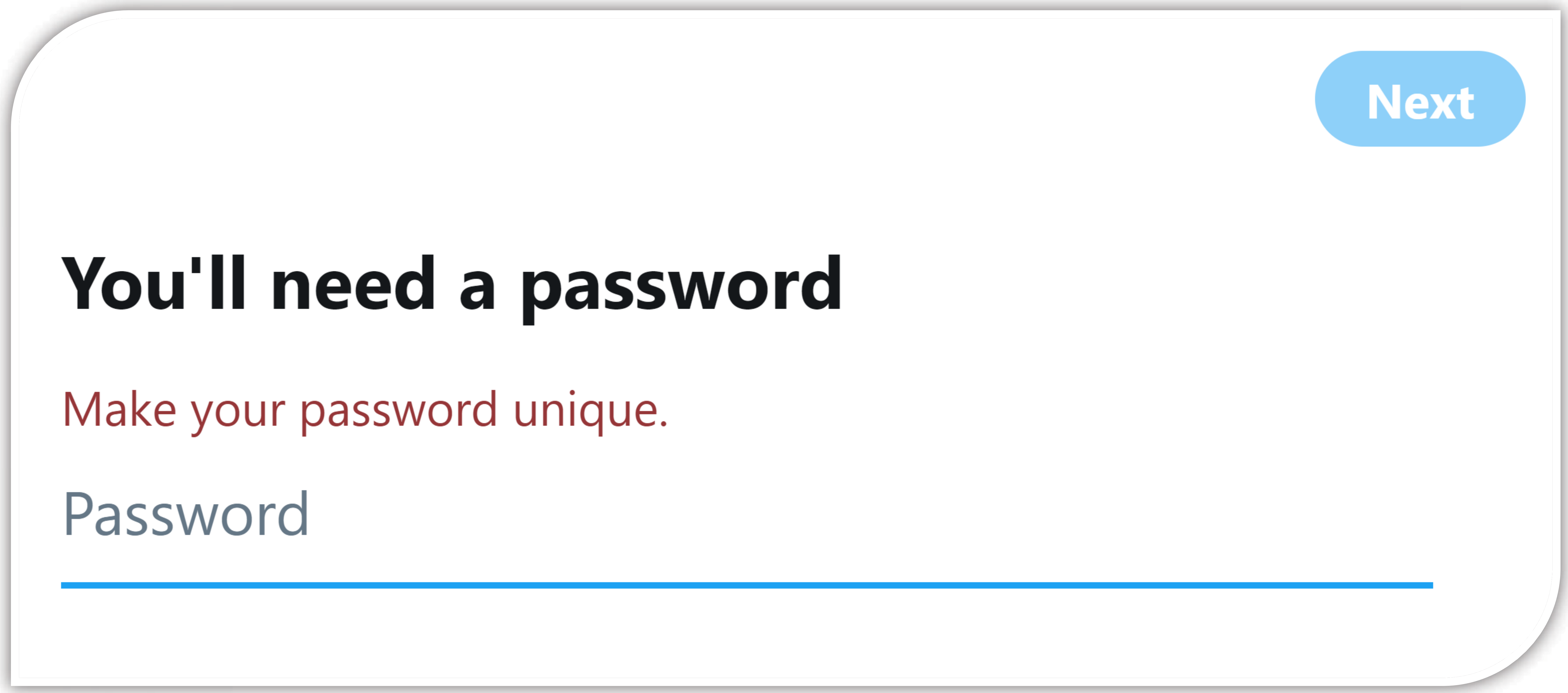
RUHR UNIVERSITÄT BOCHUM RUB

UNIVERSITY OF MARYLAND

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

Toronto, Canada | ACM CCS | October 18, 2018

use unique passwords



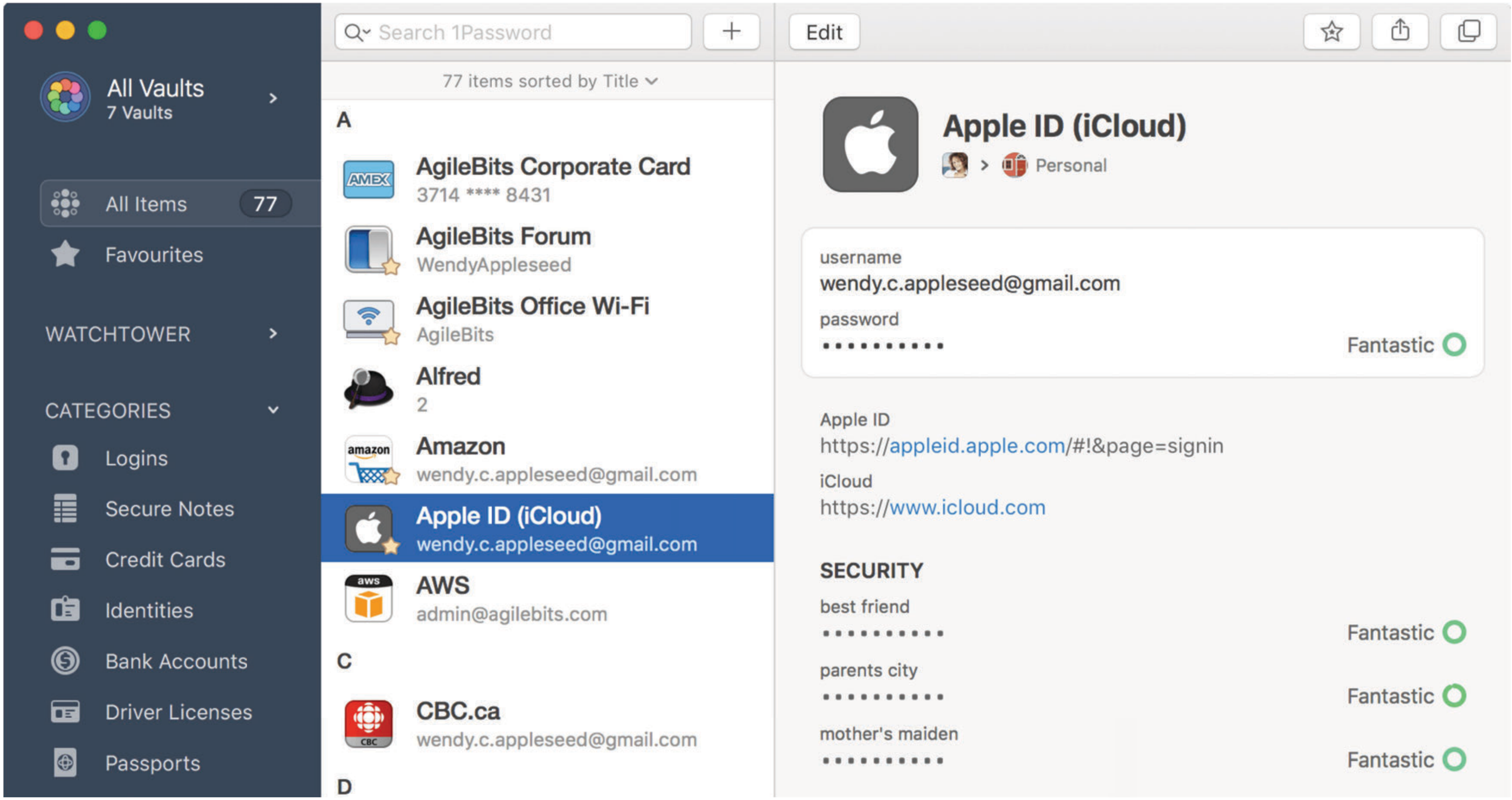
You'll need a password

Make your password unique.

Password

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

“use a password manager!”



Search 1Password

+

Edit

All Vaults
7 Vaults

All Items 77

Favourites

WATCHTOWER

CATEGORIES

Logins

Secure Notes

Credit Cards

Identities

Bank Accounts

Driver Licenses

Passports

77 items sorted by Title

A

AgileBits Corporate Card
3714 **** 8431

AgileBits Forum
WendyAppleseed

AgileBits Office Wi-Fi
AgileBits

Alfred
2

Amazon
wendy.c.appleseed@gmail.com

Apple ID (iCloud)
wendy.c.appleseed@gmail.com

AWS
admin@agilebits.com

C

CBC.ca
wendy.c.appleseed@gmail.com

D

Apple ID (iCloud)

Personal

username
wendy.c.appleseed@gmail.com

password
••••••••••• Fantastic

Apple ID
https://appleid.apple.com/#!&page=signin

iCloud
https://www.icloud.com

SECURITY

best friend
••••••••••• Fantastic

parents city
••••••••••• Fantastic

mother's maiden
••••••••••• Fantastic

people reuse passwords

R0cky!14

R0cky!17

R0cky!17

123456

Rocky!16

R0ckyStar

R0ckyBox

R0cky!17

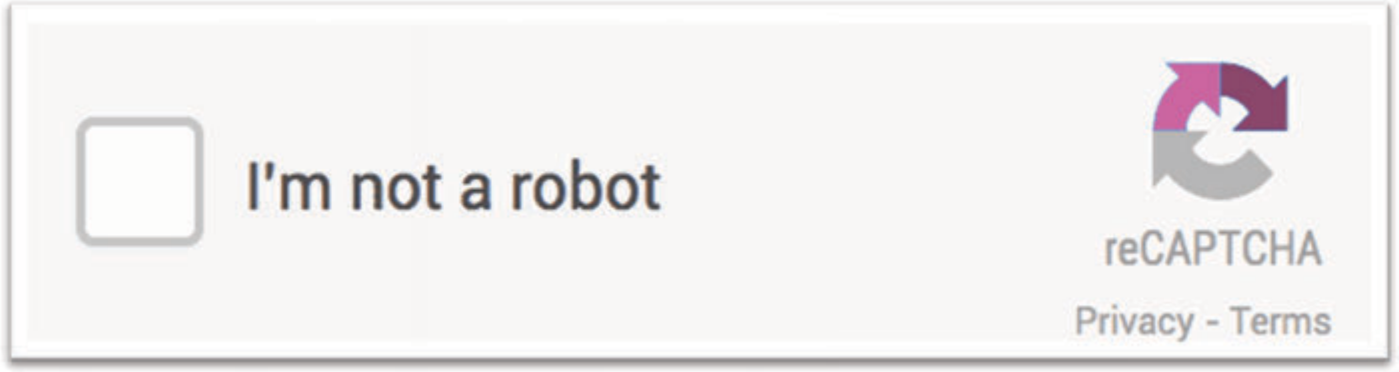
R0cky!17

AcmeCo

Memory-Hard Hash Function ✓

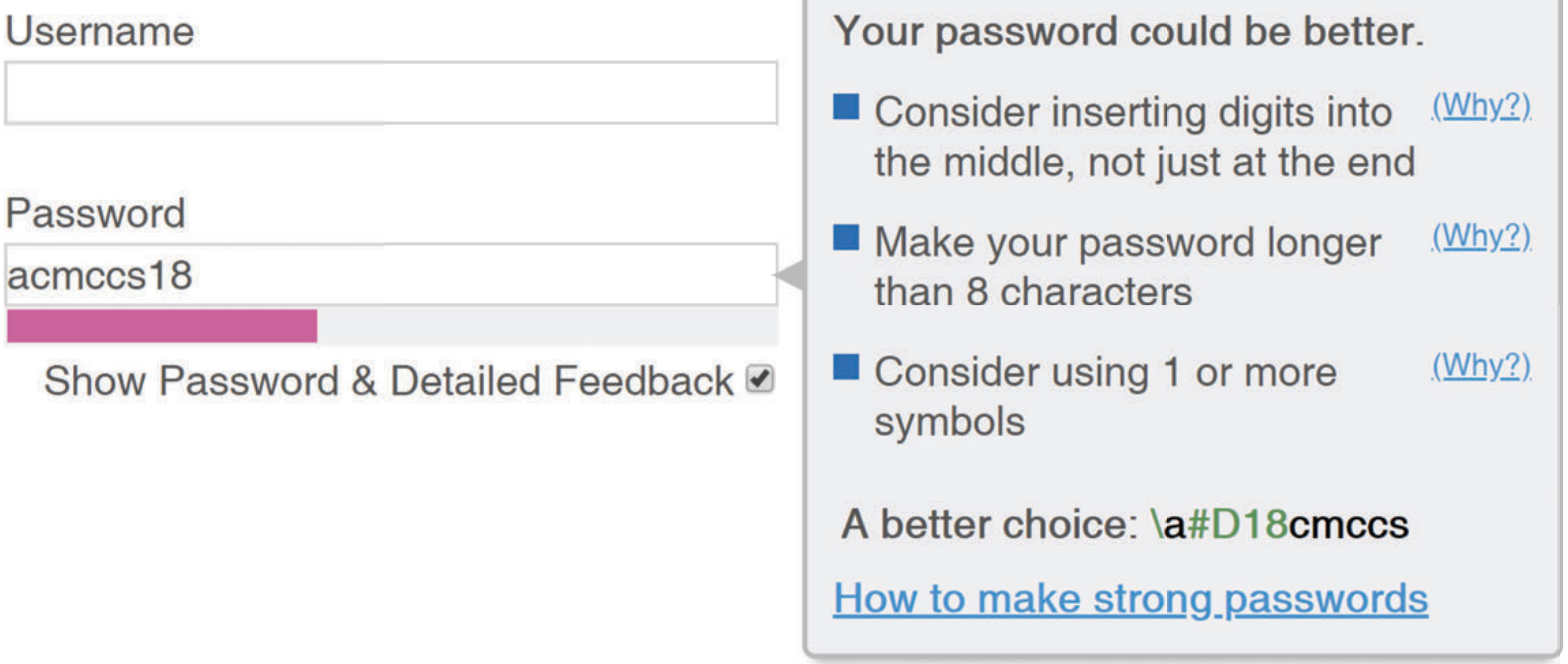
Email	Argon2i Hash of Password
…	…
jim@mail.com	$argon2i$v=19$m=4096,…
…	…

Rate-Limiting Guessing ✓



□ I'm not a robot

Password Strength Meter ✓



Username

Password

acmccs18

Show Password & Detailed Feedback ☑

Your password could be better.

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

A better choice: \a#D18cmccs

How to make strong passwords

AcmeCo

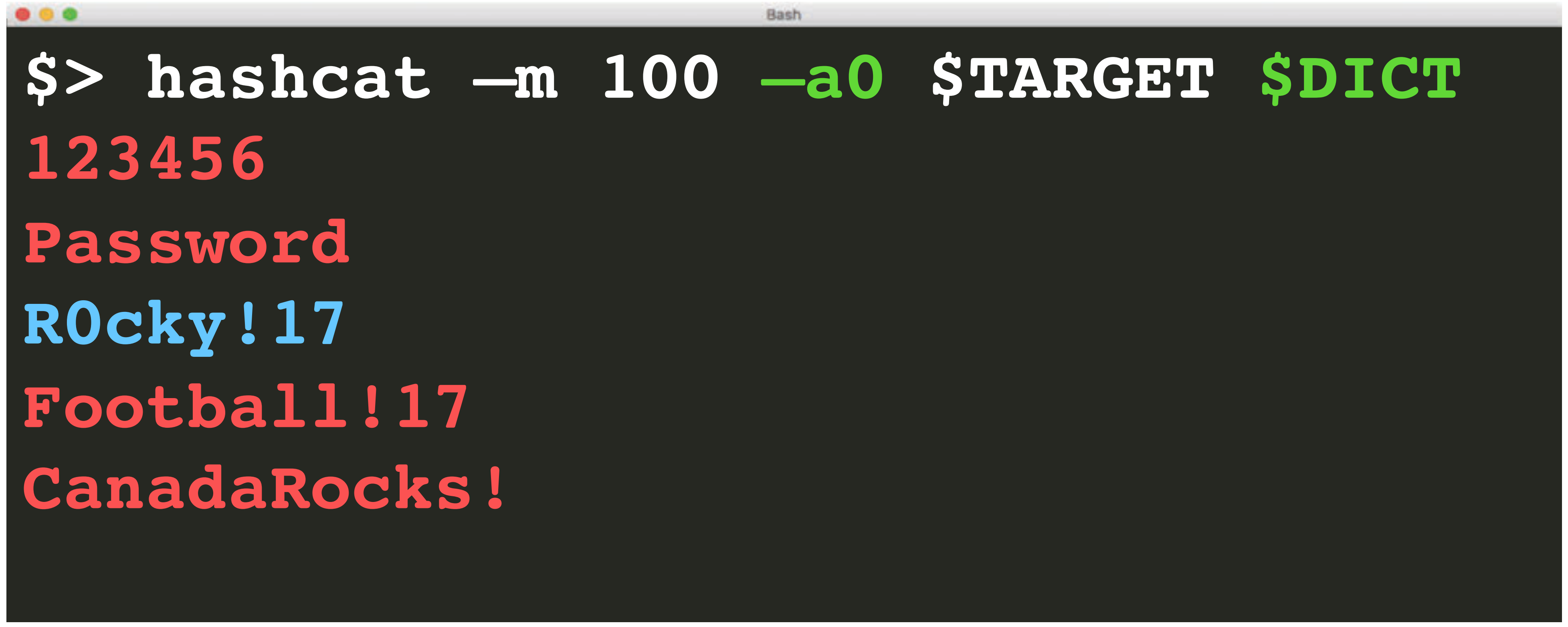
Email
...
jim@mail.com
...

LinkedIn

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

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!



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

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

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

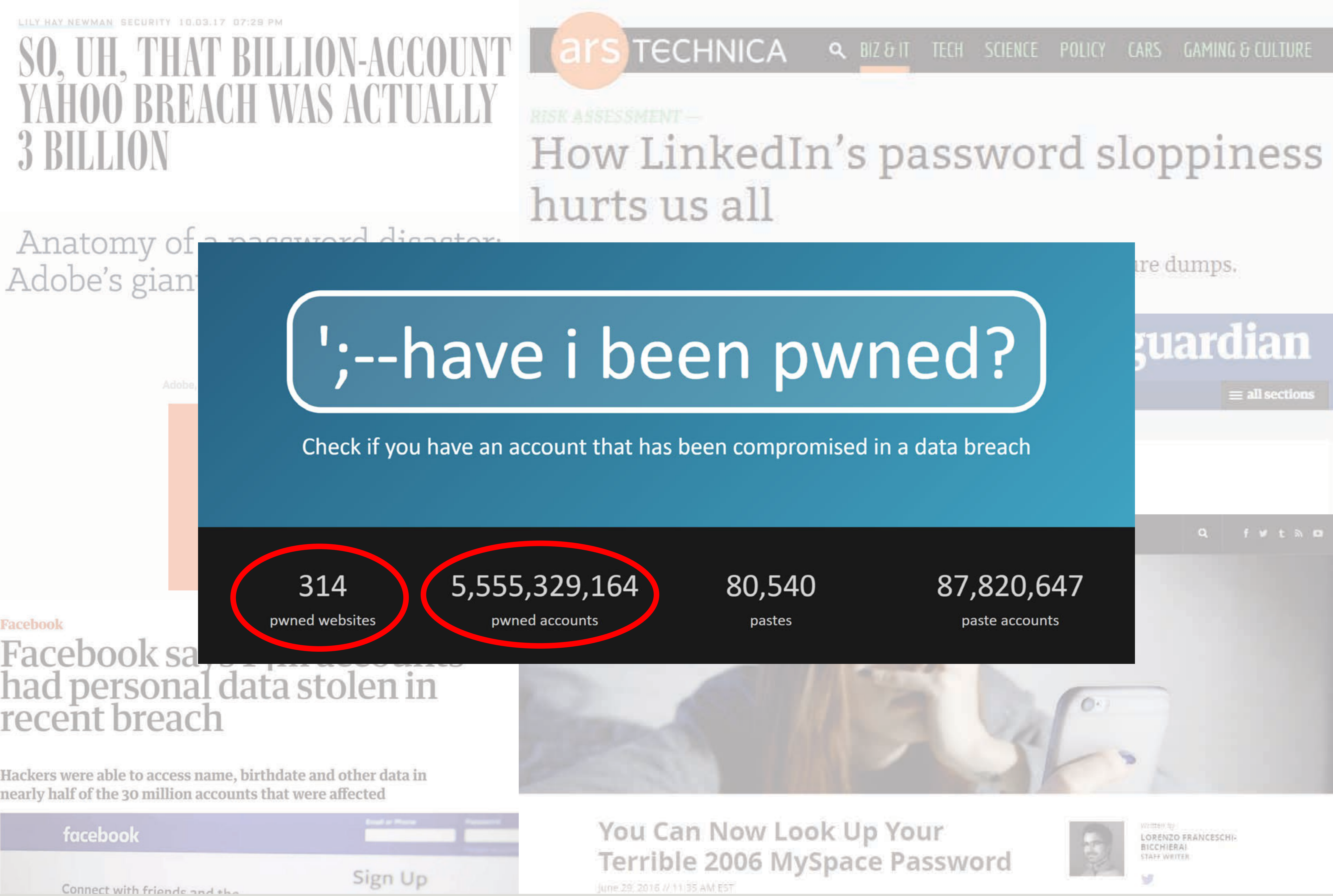
AcmeCo

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

RISK ASSESSMENT —

How LinkedIn's password sloppiness hurts us all

re dumps.

Anatomy of a password disaster: Adobe's gian

';--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 had personal data stolen in recent breach

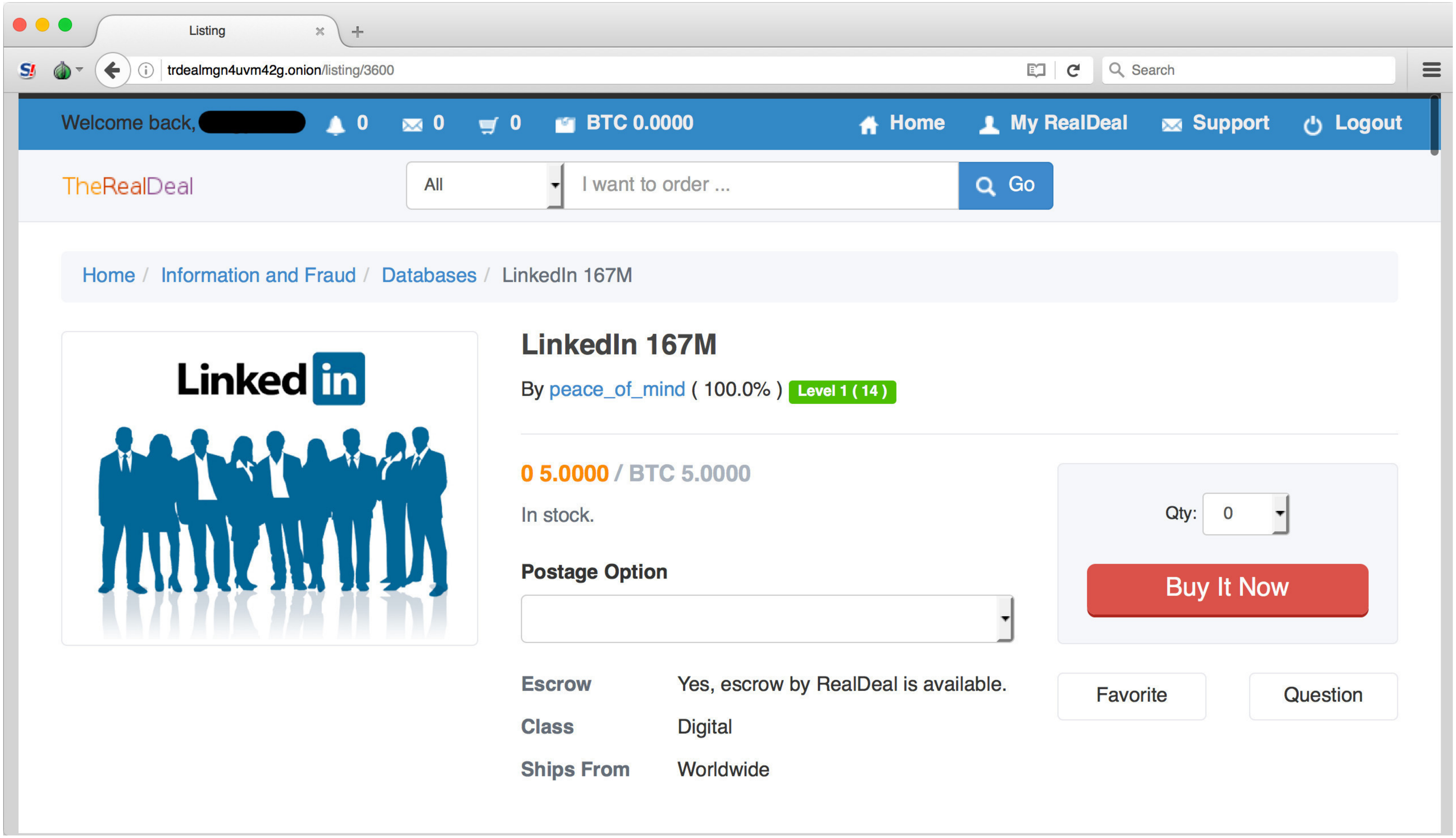
Hackers were able to access name, birthdate and other data in nearly half of the 30 million accounts that were affected

You Can Now Look Up Your Terrible 2006 MySpace Password

June 29, 2016 // 11:35 AM EST

Written by LORENZO FRANCESCHI-BICCHIERAI STAFF WRITER

black market monitoring



Listing

trdealmgn4uvm42g.onion/listing/3600

Welcome back, [redacted] 0 0 0 BTC 0.0000 Home My RealDeal Support Logout

TheRealDeal

All I want to order ... Go

Home / Information and Fraud / Databases / LinkedIn 167M

LinkedIn 167M

By peace_of_mind (100.0%) Level 1 (14)

0 5.0000 / BTC 5.0000

In stock.

Postage Option

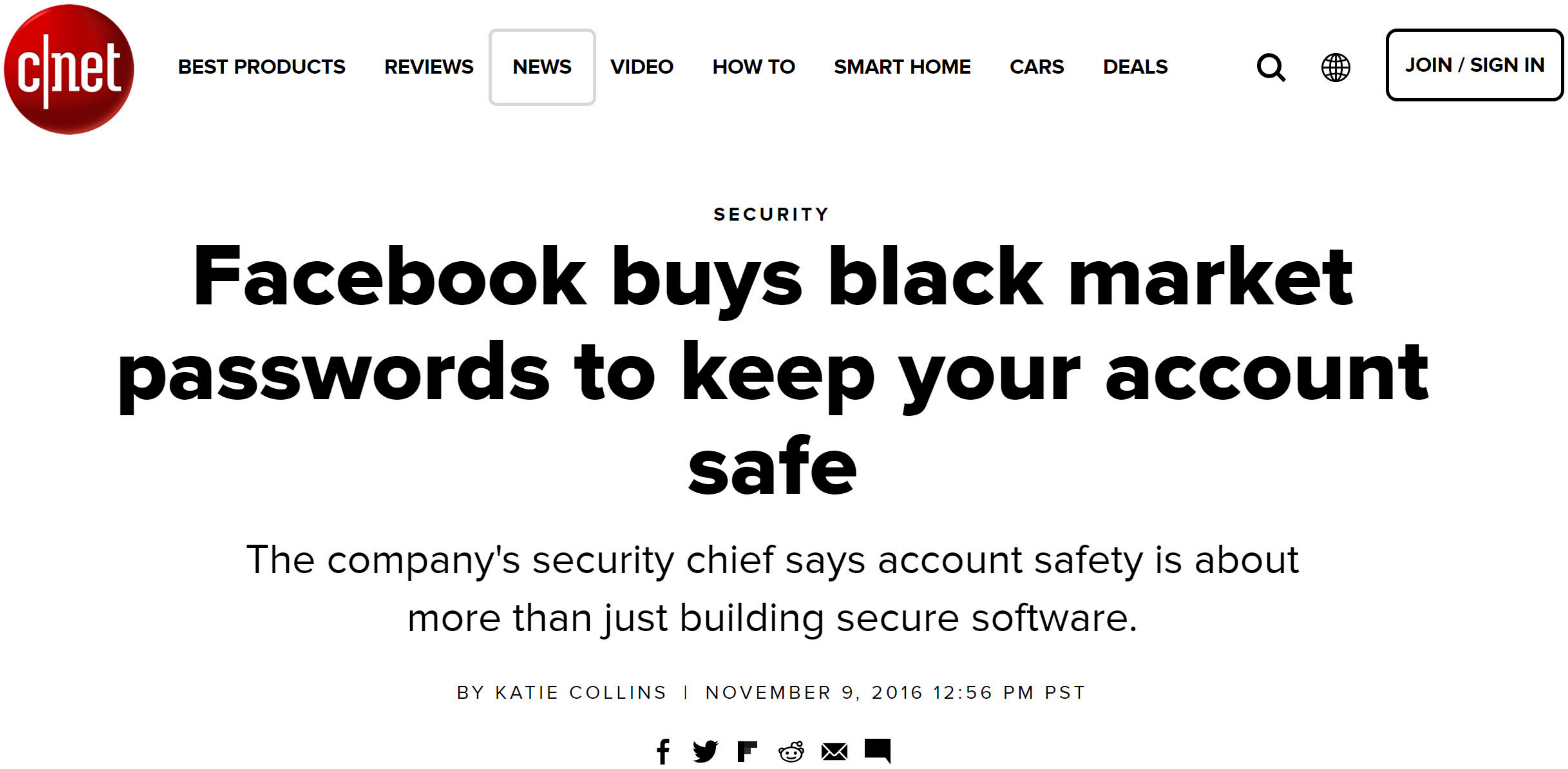
Qty: 0

Buy It Now

Favorite Question

Escrow	Yes, escrow by RealDeal is available.
Class	Digital
Ships From	Worldwide

black market monitoring



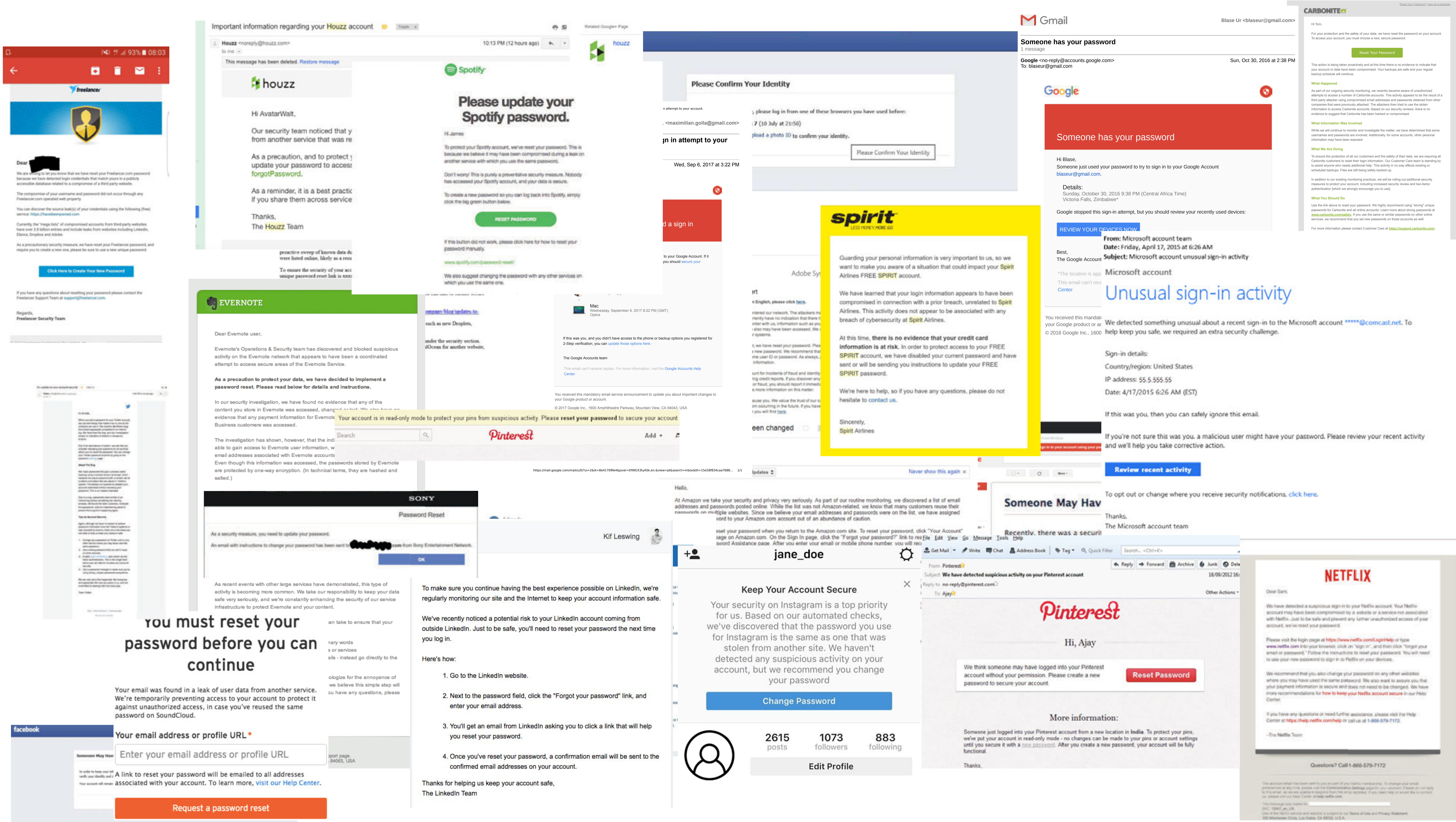
SECURITY

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?



Important information regarding your Houzz account

houzz

Hi AvatarWalt,

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

As a precaution, and to protect y update your password to acces forgotPassword.

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

Thanks,
The Houzz Team

Spotify

Please update your Spotify password.

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 so you can log back into Spotify, simply click the big green button below.

RESET PASSWORD

Please Confirm Your Identity

Gmail

Someone has your password

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

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:

REVIEW YOUR DEVICES NOW

CARBONITE

freelancer

Dear [redacted]

Click Here to Create Your New Password

Regards,
Freelancer Security Team

EVERNOTE

Dear Evernote user,

Evernote's Operations & Security team has discovered and blocked suspicious activity on the Evernote network that appears to have been a coordinated attempt to access secure areas of the Evernote Service.

As a precaution to protect your data, we have decided to implement a password reset. Please read below for details and instructions.

spirit

Guarding your personal information is very important to us, so we want to make you aware of a situation that could impact your Spirit Airlines FREE SPIRIT account.

We have learned that your login information appears to have been compromised in connection with a prior breach, unrelated to Spirit Airlines. This activity does not appear to be associated with any breach of cybersecurity at Spirit Airlines.

At this time, there is no evidence that your credit card information is at risk. In order to protect access to your FREE SPIRIT account, we have disabled your current password and have sent or will be sending you instructions to update your FREE SPIRIT password.

We're here to help, so if you have any questions, please do not hesitate to contact us.

Sincerely,
Spirit Airlines

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

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

Your account is in read-only mode to protect your pins from suspicious activity. Please reset your password to secure your account

Pinterest

SONY

Password Reset

As a security measure, you need to update your password.

OK

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

Someone May Hav

You must reset your password before you can continue

Your email was found in a leak of user data from another service. We're temporarily preventing access to your account to protect it against unauthorized access, in case you've reused the same password on SoundCloud.

Your email address or profile URL *

Enter your email address or profile URL

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

Kif Leswing

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

jane_doe

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

Edit Profile

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

Pinterest

Hi, Ajay

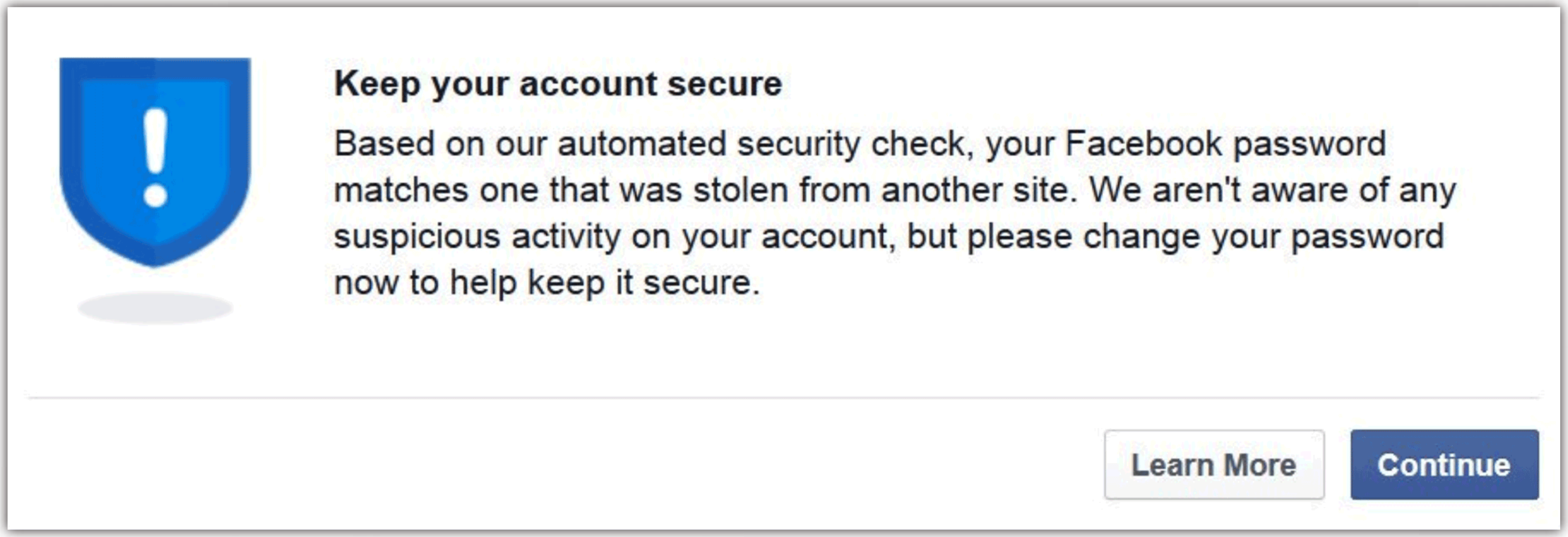
We think someone may have logged into your Pinterest account without your permission. Please create a new password to secure your account.

Reset Password

More information:

NETFLIX

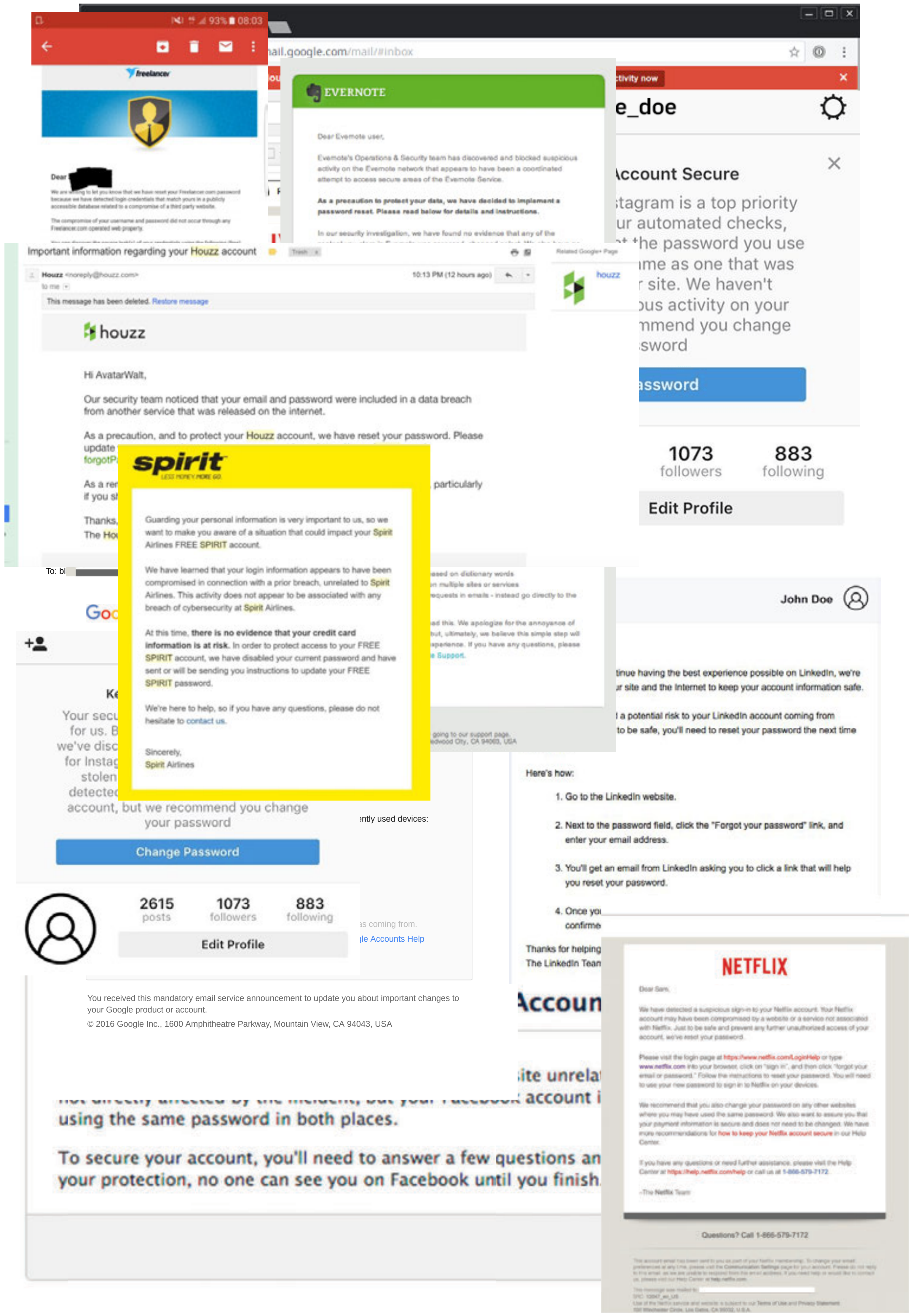
Questions? Call 1-866-579-7172



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.

24 notifications



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.

Dear Evernote user,

Evernote's Operations & Security team has discovered and blocked suspicious activity on the Evernote network that appears to have been a coordinated attempt to access secure areas of the Evernote Service.

As a precaution to protect your data, we have decided to implement a password reset. Please read below for details and instructions.

In our security investigation, we have found no evidence that any of the

ccount Secure

stagram is a top priority
ur automated checks,
the password you use
ame as one that was
r site. We haven't
ous activity on your
mmend you change
ssword

assword

1073 followers 883 following

Edit Profile

Important information regarding your Houzz account Trash

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

This message has been deleted. Restore message

Related Google+ Page
houzz

Hi AvatarWalt,

Our security team noticed that your email and password were included in a data breach from another service that was released on the internet.

As a precaution, and to protect your Houzz account, we have reset your password. Please update
forgotP

As a ren
if you sh
particularly

Thanks,
The Hou

Guarding your personal information is very important to us, so we want to make you aware of a situation that could impact your Spirit Airlines FREE SPIRIT account.

We have learned that your login information appears to have been compromised in connection with a prior breach, unrelated to Spirit Airlines. This activity does not appear to be associated with any breach of cybersecurity at Spirit Airlines.

At this time, **there is no evidence that your credit card information is at risk.** In order to protect access to your FREE SPIRIT account, we have disabled your current password and have sent or will be sending you instructions to update your FREE SPIRIT password.

We're here to help, so if you have any questions, please do not hesitate to contact us.

Sincerely,
Spirit Airlines

To: bl

ased on dictionary words
n multiple sites or services
equests in emails - instead go directly to the

ad this. We apologize for the annoyance of
but, ultimately, we believe this simple step will
xperience. If you have any questions, please
e Support.

going to our support page.
edwood City, CA 94063, USA

Ke

Your secu
for us. B
we've disc
for Instag
stolen
detecte
account, but we recommend you change your password

Change Password

2615 posts 1073 followers 883 following

Edit Profile

ently used devices:

as coming from.
gle Accounts Help

You received this mandatory email service announcement to update you about important changes to your Google product or account.

© 2016 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

John Doe

tinue having the best experience possible on LinkedIn, we're
r site and the Internet to keep your account information safe.

a potential risk to your LinkedIn account coming from
to be safe, you'll need to reset your password the next time

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 yo
confirme

Thanks for helping
The LinkedIn Tean

Accoun

ite unrela
not directly affected by the incident, but your Facebook account i
using the same password in both places.

To secure your account, you'll need to answer a few questions an
your protection, no one can see you on Facebook until you finish

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

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 at any time, please visit the Communication Settings page for your account. Please do not reply to this email, as we are unable to respond from this email address. If you need help or would like to contact us, please visit our Help Center at help.netflix.com.

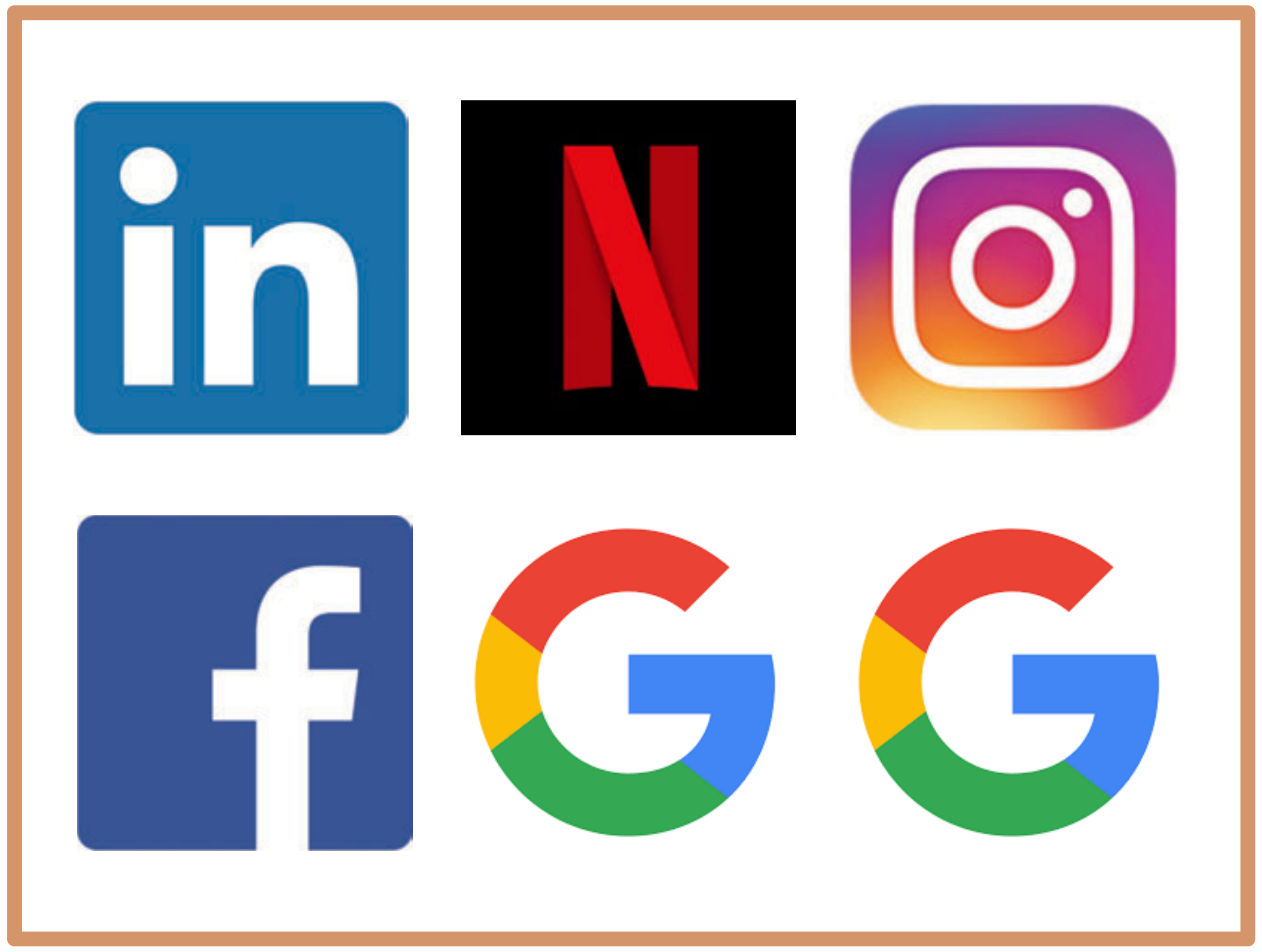
This message was mailed to

SRC: 13047_en_US

Use of the Netflix service and website is subject to our Terms of Use and Privacy Statement.

100 Winchester Circle, Los Gatos, CA 95032, U.S.A.

6 representative notifications



methodology

STUDY 1

previously sent password-reuse notifications

STUDY 2

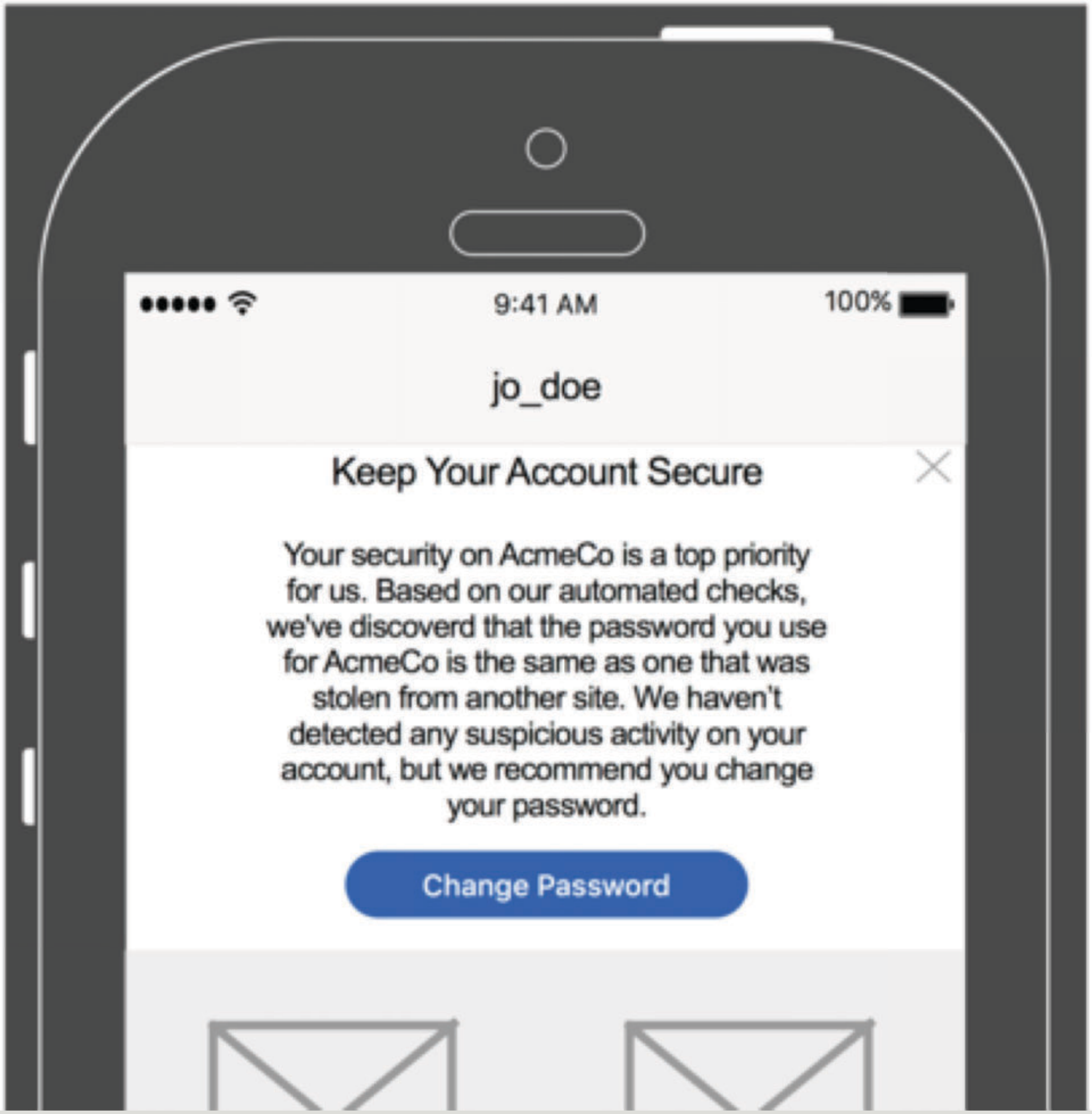
individual components of password-reuse notifications

STUDY 1

Imagine you have an important account with AcmeCo…

1

AcmeCo notifications



Keep Your Account Secure

Your security on AcmeCo is a top priority for us. Based on our automated checks, we've discoverd that the password you use for AcmeCo 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.

1

questions asked

notification understanding

feelings

actions

perceptions

demographics

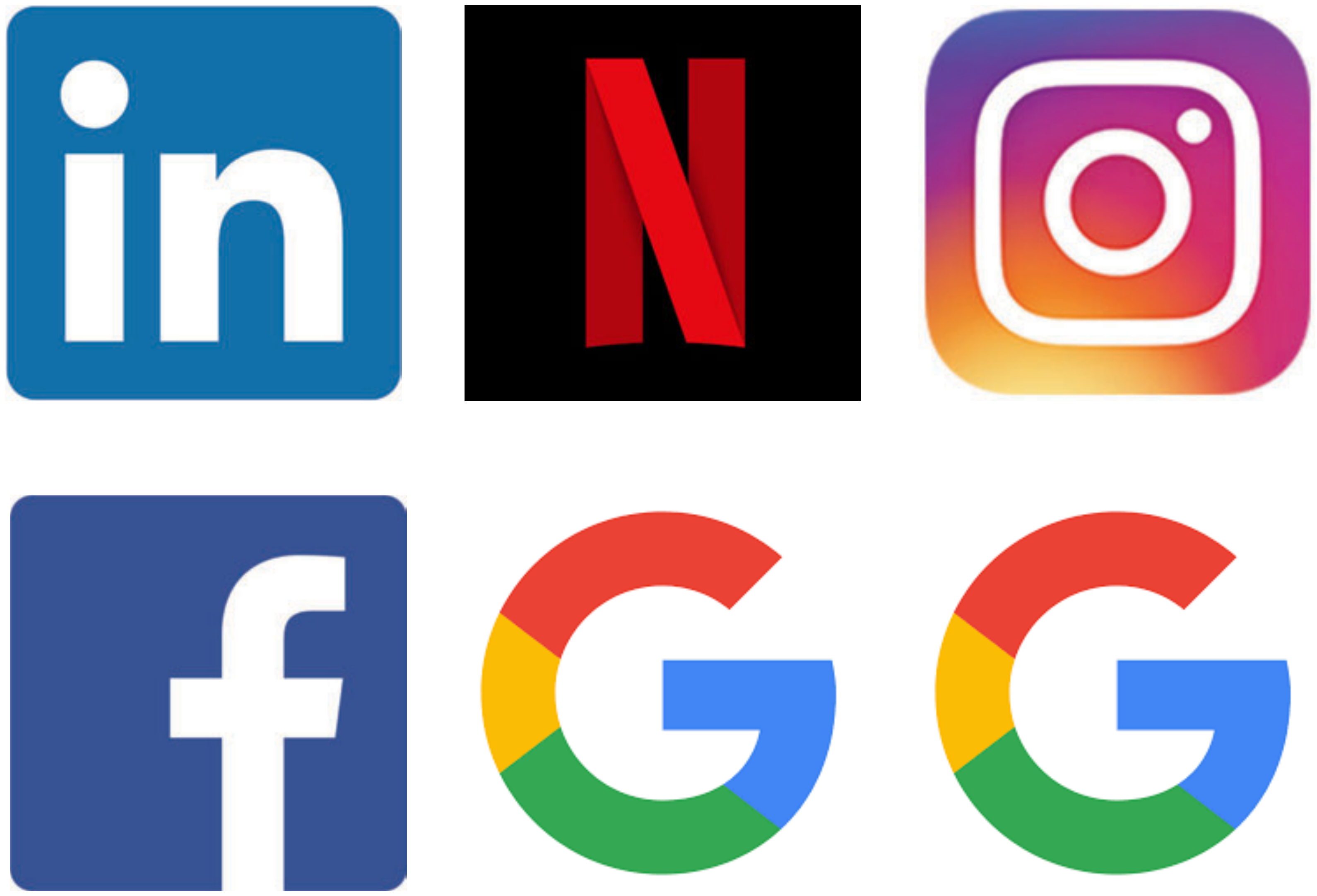
1

survey setup

180 respondents

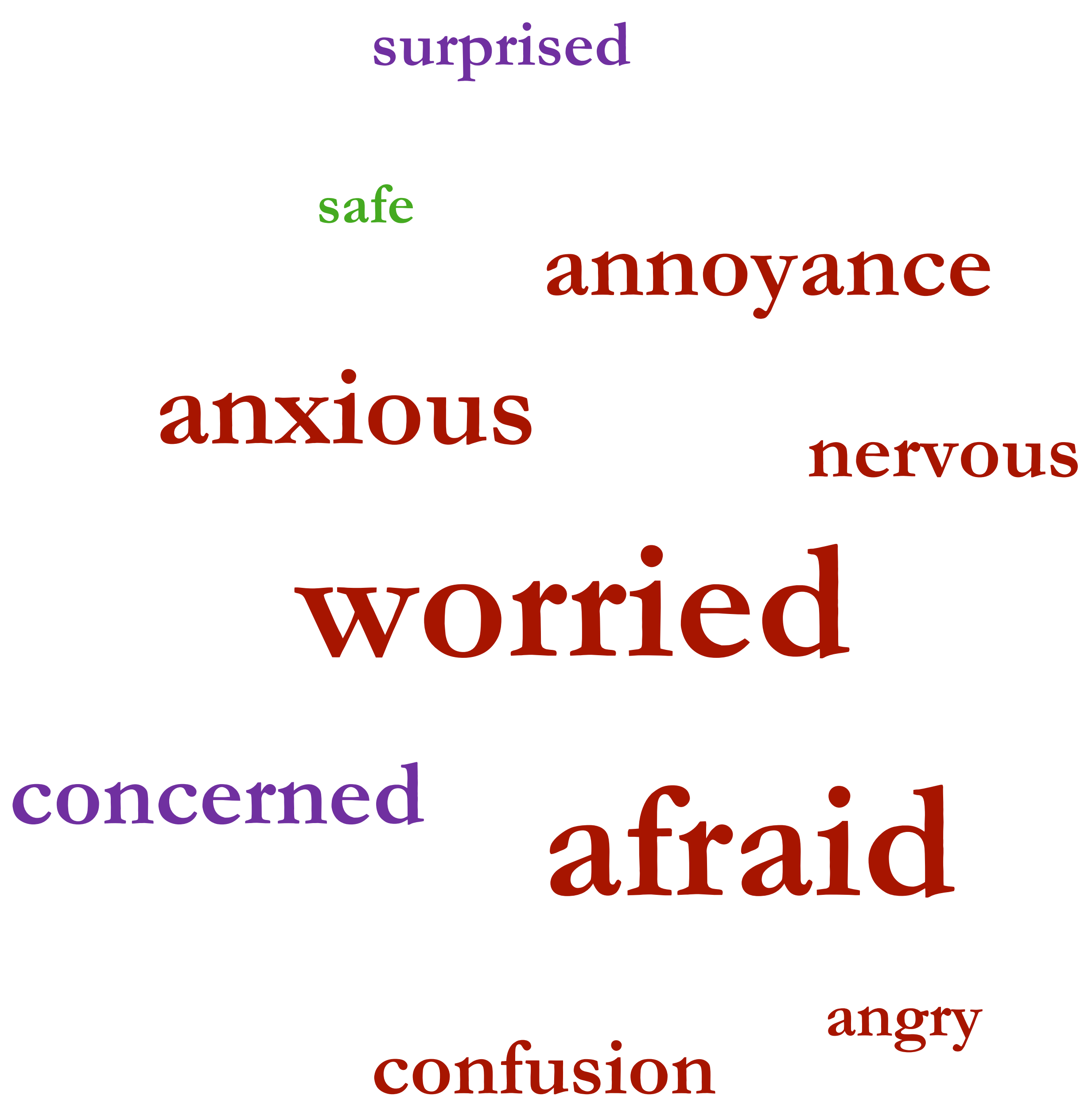
- Amazon MTurk
- 15 mins
- Compensated $2.50

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

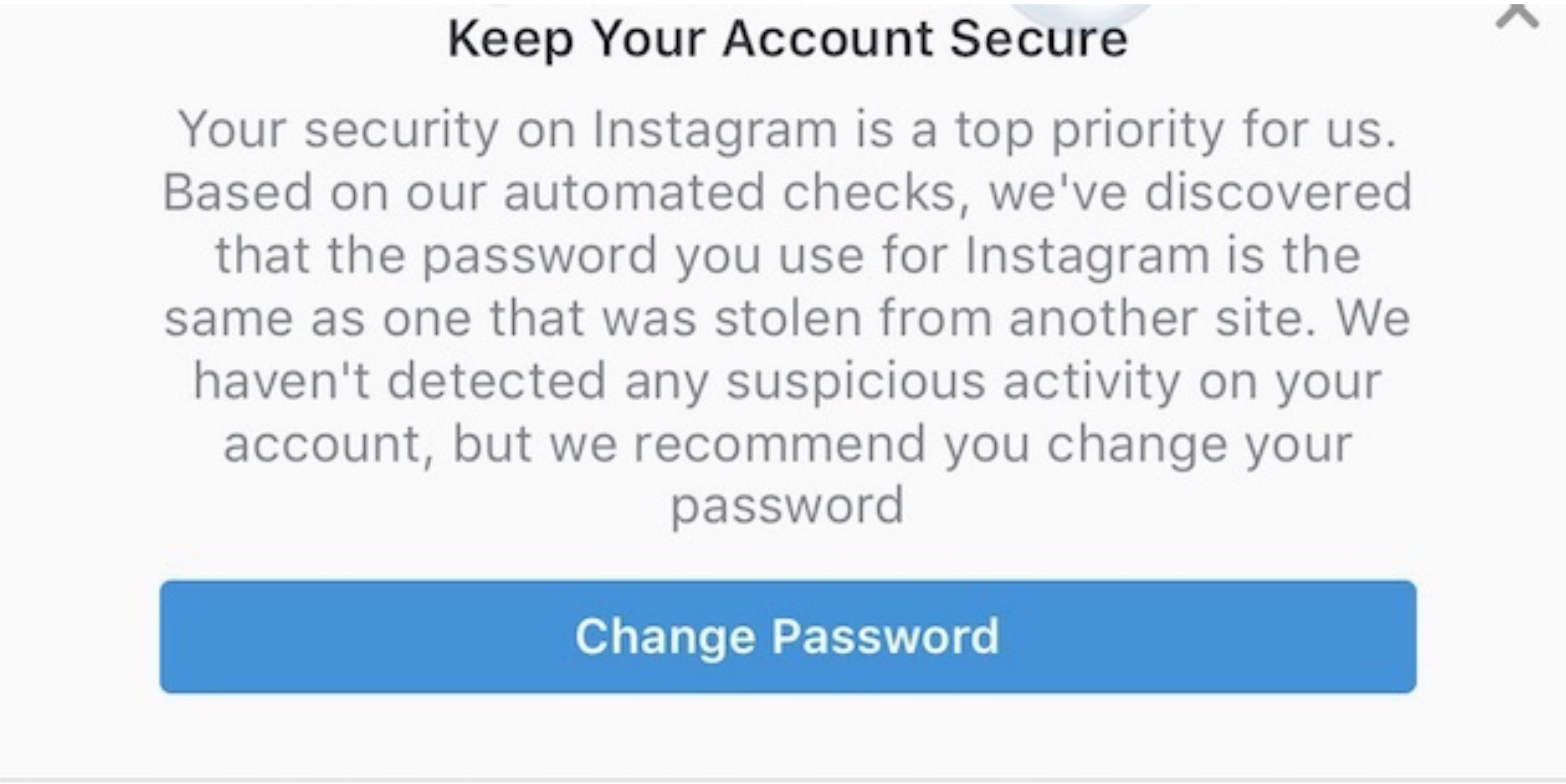
0 - 4%
respondents

allude to

password reuse

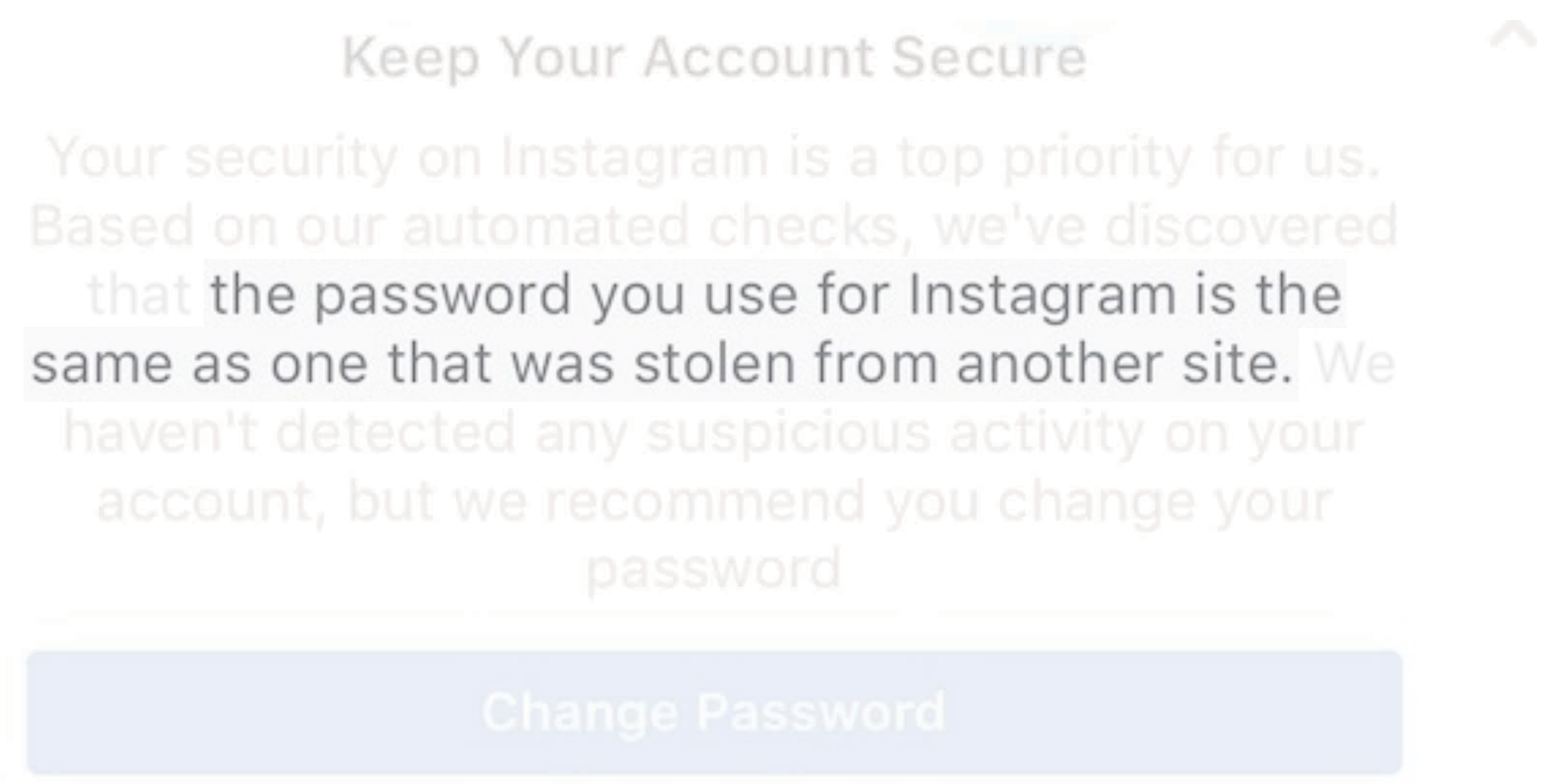
48 - 56%
respondents

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



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

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

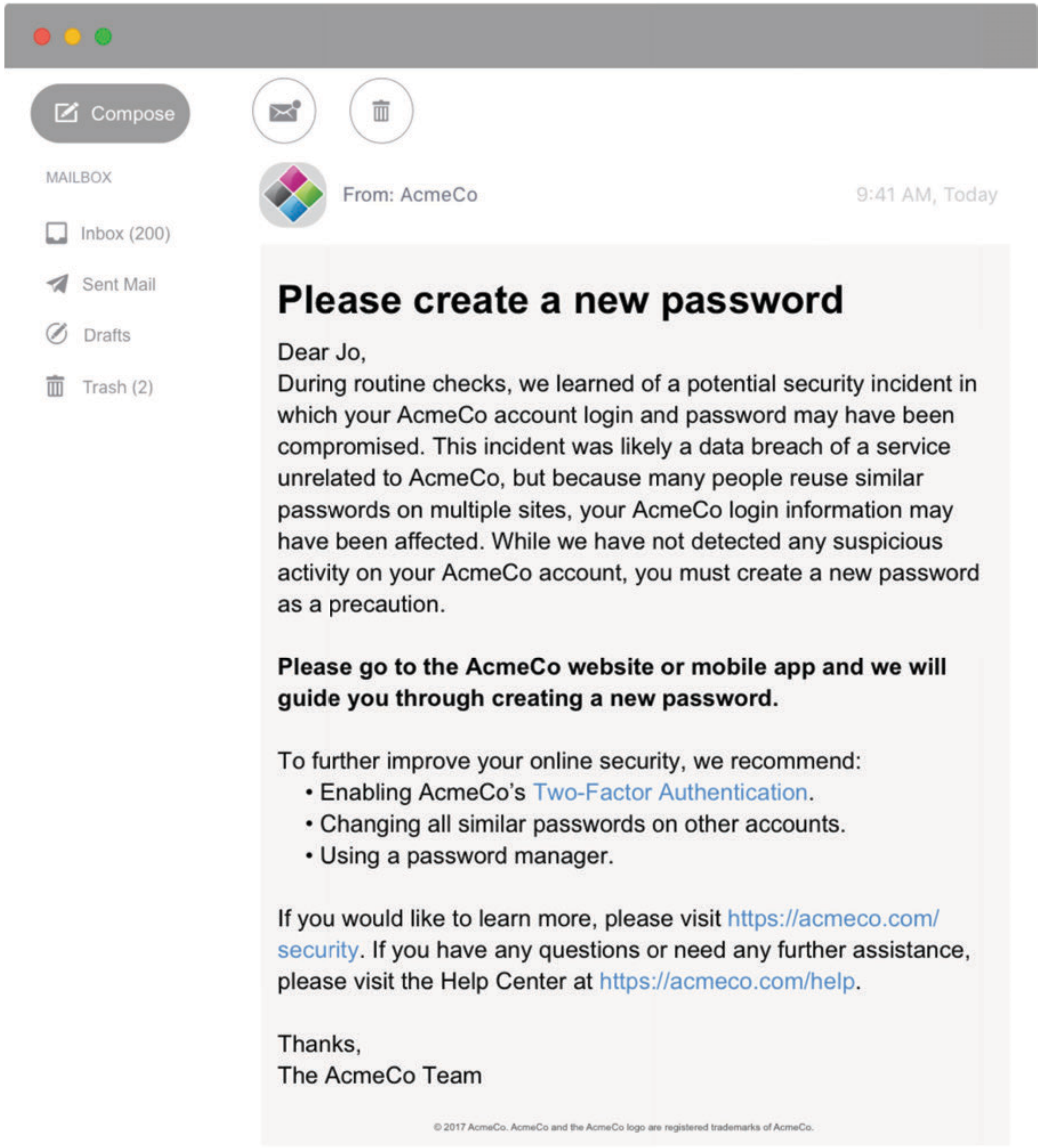
secure actions

legitimate

trust

STUDY 2

our model notification



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 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.

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

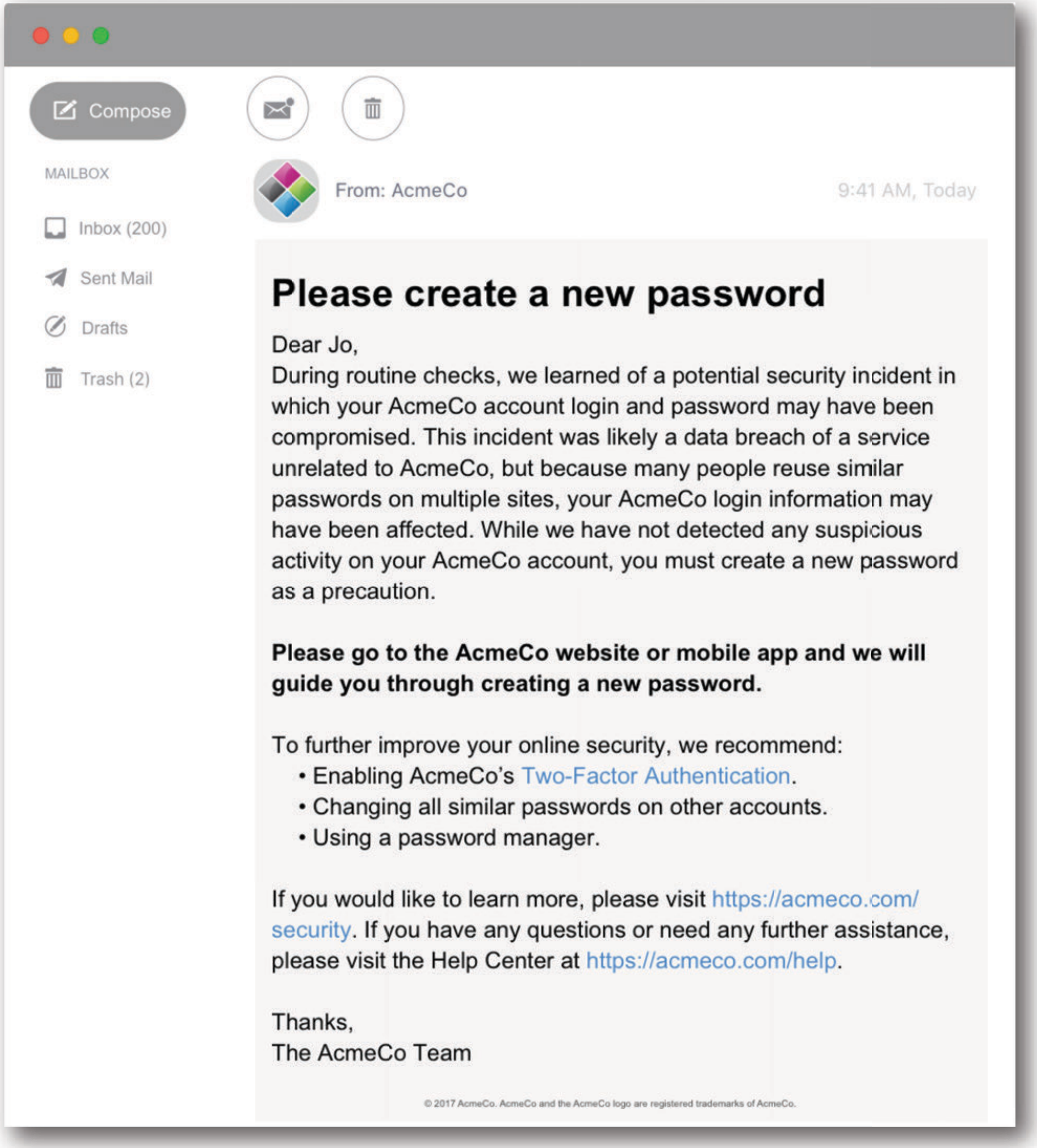
send via email + more immediate channel

name password reuse as root cause

force password reset

encourage 2FA and password managers

suggest unique passwords for other accounts



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.

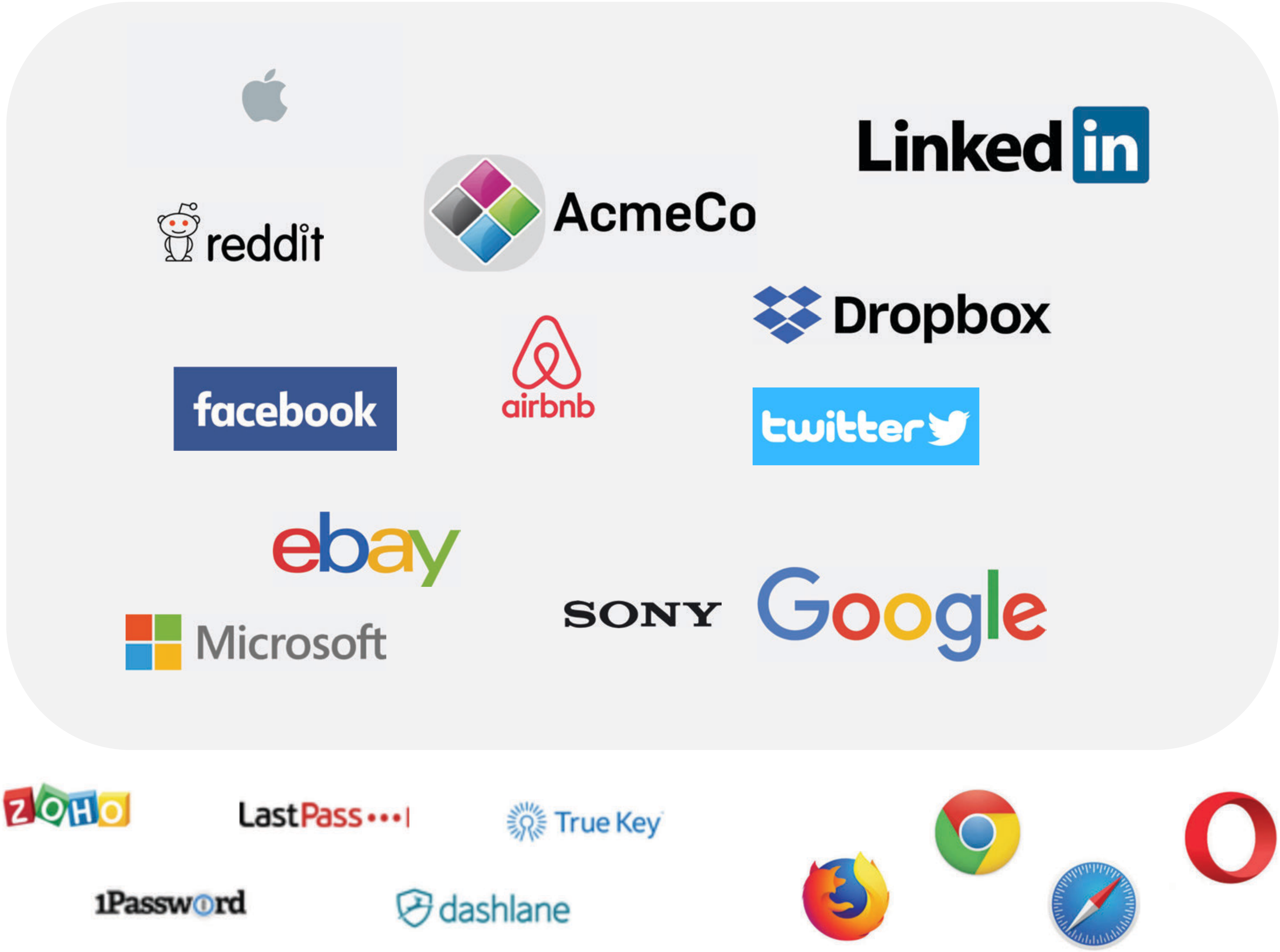
Thanks,
The AcmeCo Team

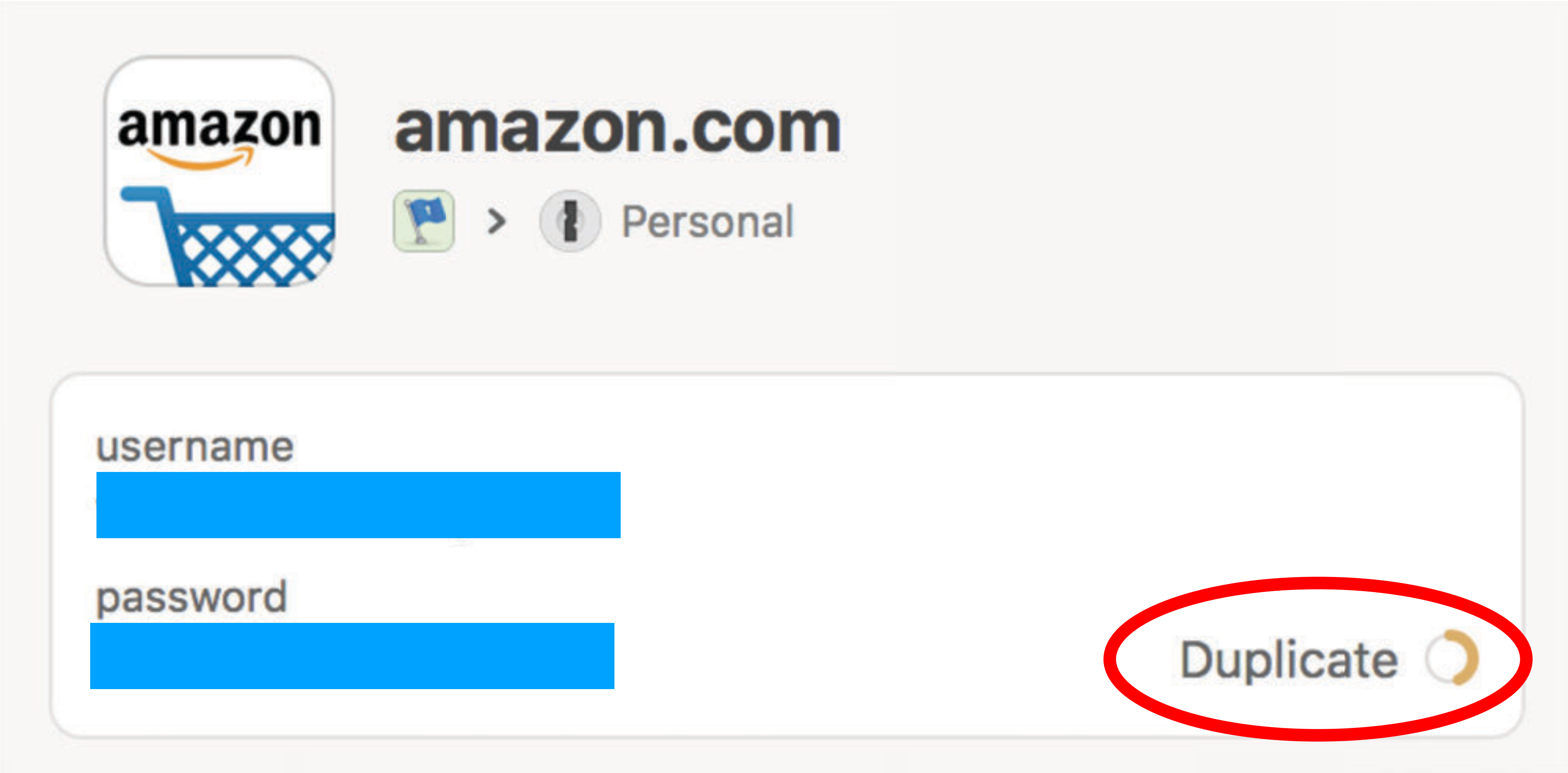
conclusion

1. formative, systematic study of password-reuse notifications

2. developed best practices

3. future work should study novel notifications


reddit
AcmeCo
Linked in
Dropbox
facebook
airbnb
twitter
ebay
Microsoft
SONY
Google
ZOHO
LastPass
True Key
1Password
dashlane



amazon.com

Personal

username

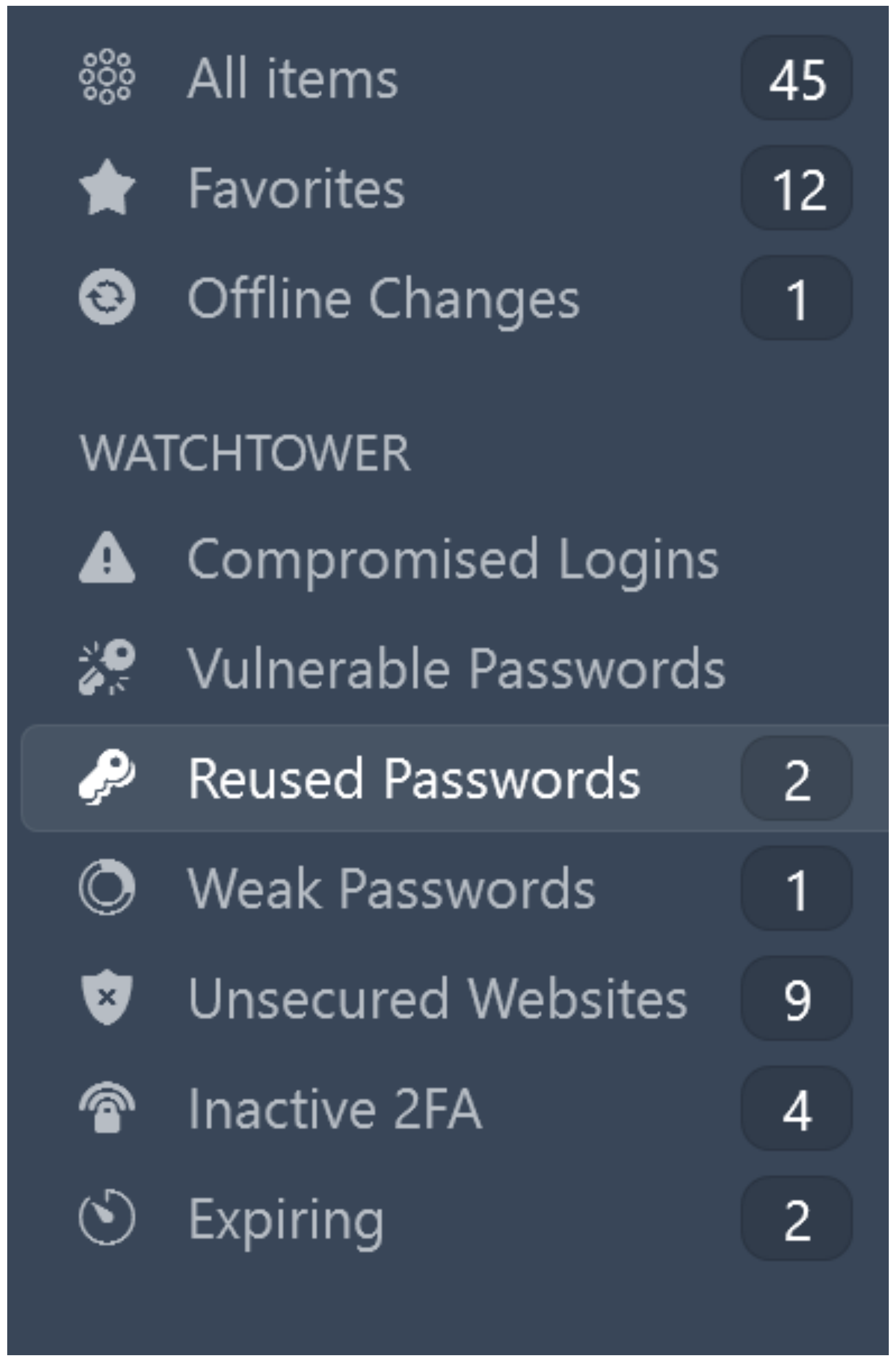
[redacted]

password

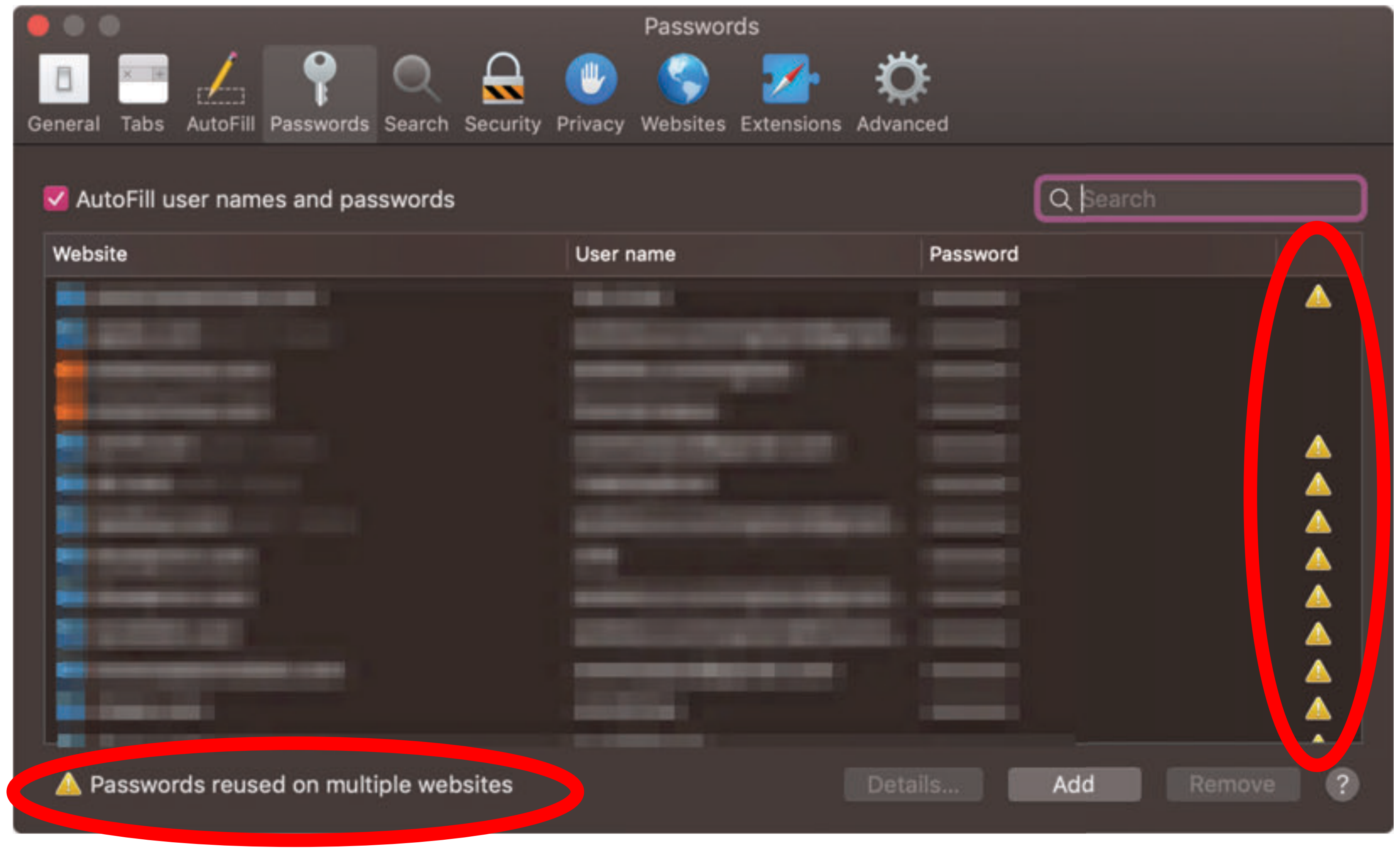
[redacted]

Duplicate

1Password



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



☑ AutoFill user names and passwords

Website	User name	Password

⚠ Passwords reused on multiple websites

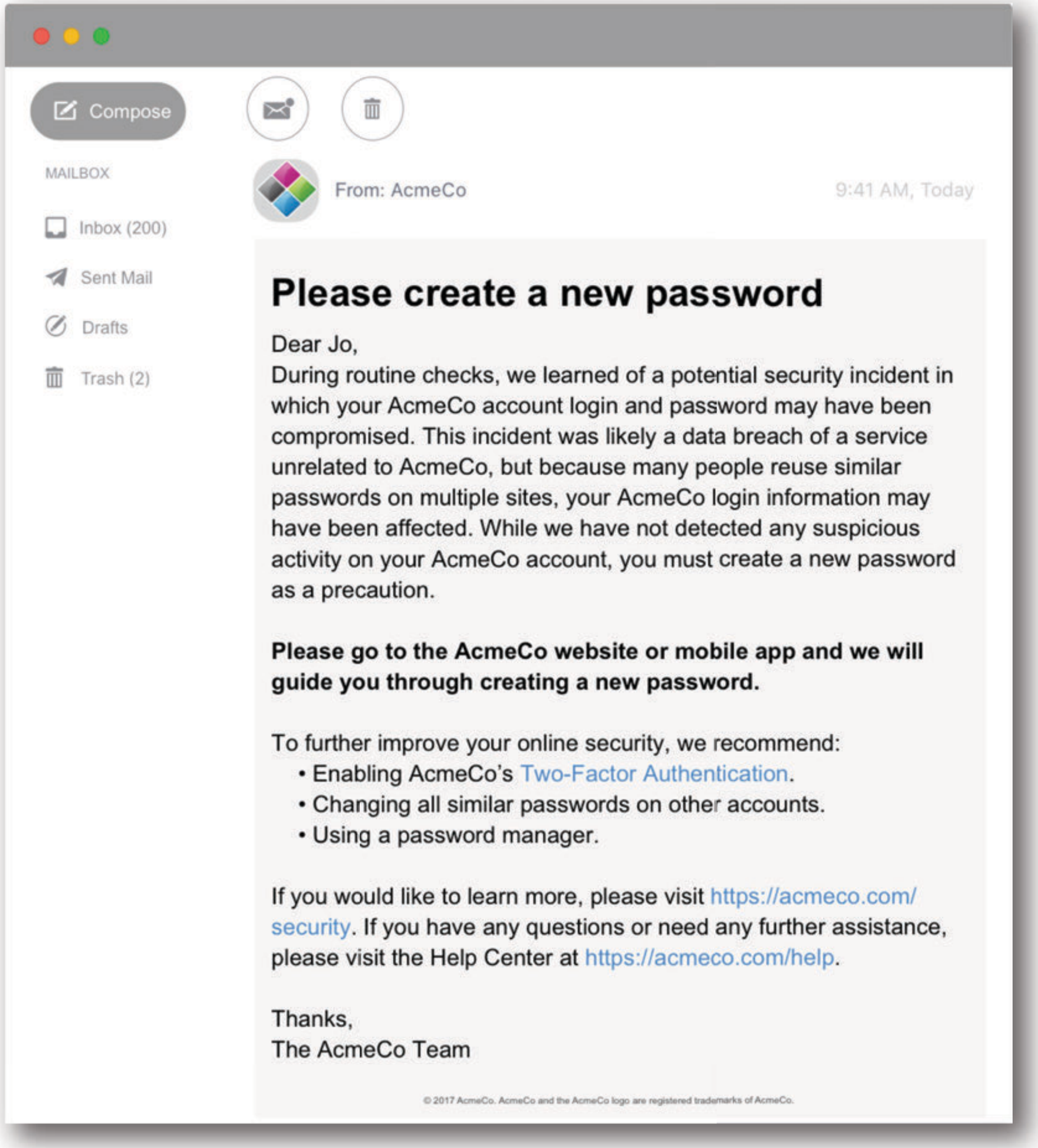
macOS Mojave, Safari 12

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



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

THE UNIVERSITY OF CHICAGO

RUHR UNIVERSITÄT BOCHUM RUB

UNIVERSITY OF MARYLAND

SUPER GROUP Security, Usability, & Privacy Education & Research