Everything but the User: Reducing Password Reuse

Miranda Wei, The University of Chicago

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

the password is dead

Bill Gates
2004

[IMG: Bill Gates by devos on Flickr]

the password is dead

"There is no doubt that over time, people are going to rely less and less on passwords. People use the same password on different systems, they write them down and they just don't meet the challenge for anything you really want to secure."
-Bill Gates, 2004

the password is dead

"There is no doubt that over time, people are going to rely less and less on passwords. People use the same password on different systems, they write them down and they just don't meet the challenge for anything you really want to secure."

-Bill Gates, 2004

the password is dead

"There is no doubt that over time, people are going to rely less and less on passwords. People use the same password on different systems, they write them down and they just don't meet the challenge for anything you really want to secure."
-Bill Gates, 2004

an extremely abbreviated history of password usability

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

FIPS 112

Password Usage

Date Published: May 1985

Withdrawn: February 08, 2005

4. "User-Friendly" Passwords

To assist users in remembering their passwords, the password generation algorithm should generate pass-words or passphrases that are "easy" to remember. Passwords formed by randomly choosing characters are generally difficult to remember. Passwords that are pronounceable are often easy to remember, as are passphrases that are formed by concatenating real words into a phrase or sentence.

USENIX Home • About USENIX • Events • Membership • Publications • Students

Paper - Proceedings of the 8th USENIX Security Symposium, August 23-36, 1999, Washington, D.C. [Technical Program]

Pp. 169–184 of the *Proceedings*

Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

J. D. Tygar[1]
EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu

USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

ANNE ADAMS AND MARTINA ANGELA SASSE

Confidentiality is an important aspect of computer security. It depends on authentication mechanisms, such as passwords, to safeguard access to information [9]. Traditionally, authentication procedures are divided into two stages: *identification* (User ID), to identify the user; and *authentication*, to verify that the user is the legitimate owner of the ID. It is the latter stage that requires a secret password. To date, research on password security has focused on designing technical mechanisms to protect access to systems; the usability of these mechanisms has rarely been investigated. Hitchings [8] and Davis and Price [4] argue that this narrow perspective has produced security mechanisms that are, in practice, less effective than they are generally assumed to be. Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design. It seems that currently, hackers pay more attention to the human link in the security chain than security designers do, for example, by using social engineering techniques to obtain passwords.

The key element in password security is the crackability of a password combination. Davies and Ganesan [3] argue that an adversary's ability to crack passwords is greater than usually believed. System-generated passwords are essentially the optimal security approach; however, user-generated passwords are potentially more memorable and thus less likely to be disclosed (because users do not have to write them down). The U.S. Federal Information Processing Standards [5] suggest several criteria for assuring different levels of password security. *Password composition*, for example, relates the size of a character set from which a password has been chosen to its level of security. An alphanumeric password is therefore more secure than one composed of letters alone. Short *password lifetime*—changing passwords frequently—is suggested as reducing the risk associated with undetected compromised passwords. Finally, *password ownership*, in particular individual ownership, is recommended to:

- Increase individual accountability;
- Reduce illicit usage;
- Allow for an establishment of system usage audit trails; and
- Reduce frequent password changes due to group membership fluctuations.

QUENTIN WEBB

Do Users' Perceptions of Password Security Match Reality?

Blase Ur, Jonathan Bees†, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor
Carnegie Mellon University, †The Pennsylvania State University
{bur, ssegreti, lbauer, nicolasc, lorrie}@cmu.edu, †jfb5406@psu.edu

Towards Implicit Visual Memory-Based Authentication

Claude Castelluccia
Inria Grenoble
claude.castelluccia@inria.fr

Markus Dürmuth and Maximilian Golla
Ruhr-University Bochum
{markus.duermuth,maximilian.golla}@rub.de

Fatma Deniz
University of California, Berkeley
fatma@berkeley.edu

Usable Security
Why Do We Need It? How Do We Get It?

M. ANGELA SASSE AND IVAN FLECHAIS

I Think, Therefore I Am: Usability and Security of Authentication Using Brainwaves *

John Chuang[1], Hamilton Nguyen[2], Charles Wang[2], and Benjamin Johnson[3]

[1]School of Information, UC Berkeley

Graphical Passwords: .earning from the First Twelve Years

Robert Biddle, Sonia Chiasson, P.C. van Oorschot
School of Computer Science
Carleton University, Ottawa, Canada
robert_biddle@carleton.ca, chiasson@scs.carleton.ca, paulv@scs.carleton.ca

Human Selection of Mnemonic Phrase-based Passwords

Cynthia Kuo
Carnegie Mellon University
cykuo@cmu.edu

Sasha Romanosky
Carnegie Mellon University
sromanos@cmu.edu

Lorrie Faith Cranor
Carnegie Mellon University
lorrie@cmu.edu

Passwords you'll never forget, but can't recall

Daphna Weinshall
School of Computer Science and Engineering
Center for Neural Computation
Hebrew University
Jerusalem, Israel

Scott Kirkpatrick
School of Engineering and Computer Scienc
Hebrew University
Jerusalem, Israel
kirk@cs.huji.ac.il

"I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab

Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor
Carnegie Mellon University
{bur, fnoma, jbees, ssegreti, rshay, lbauer, nicolasc, lorrie}@cmu.edu

Guessing human-chosen secrets

Joseph Bonneau

explosion of usable passwords research

Password Management Strategies for Online Accounts

Shirley Gaw
Department of Computer Science
Princeton University
Princeton, NJ USA
sgaw@cs.princeton.edu

Edward W. Felten
Center for Information Technology Policy
Wilson School of Public and International Affairs
Department of Computer Science
Princeton University

PassPoints: Design and longitudinal evaluation of a graphical password system

Susan Wiedenbeck[a,*], Jim Waters[a], Jean-Camille Birget[b], Alex Brodskiy[c], Nasir Memon[c]

[a]*College of Information Science & Technology, Drexel University, Philadelphia, PA 19104, USA*
[b]*Department of Computer Science, Rutgers, The State University of New Jersey, Camden, NJ 08102, USA*
[c]*Department of Co*

A Usability Study and Critique of Two Password Managers *

Sonia Chiasson and P.C. van Oorschot
of Computer Science, Carleton University, Ottawa, Canada
chiasson@scs.carleton.ca

Oriented Techn

Let's go in for a closer look: Observing passwords in their natural habitat

Sarah Pearman* Jeremy Thomas* Pardis Emani Naeini*
Hana Habib* Lujo Bauer* Nicolas Christin*
Lorrie Faith Cranor* Serge Egelman† Alain Forget‡

gie Mellon University, †International Computer Science Institute, ‡Google, Inc.
{spearman,thomasjm,pardis,hana007,lbauer,nicolasc,lorrie}@cmu.edu
egelman@icsi.berkeley.edu
aforget@google.com

A Spoonful of Sugar? The Impact of Guidance and Feedback on Password-Creation Behavior

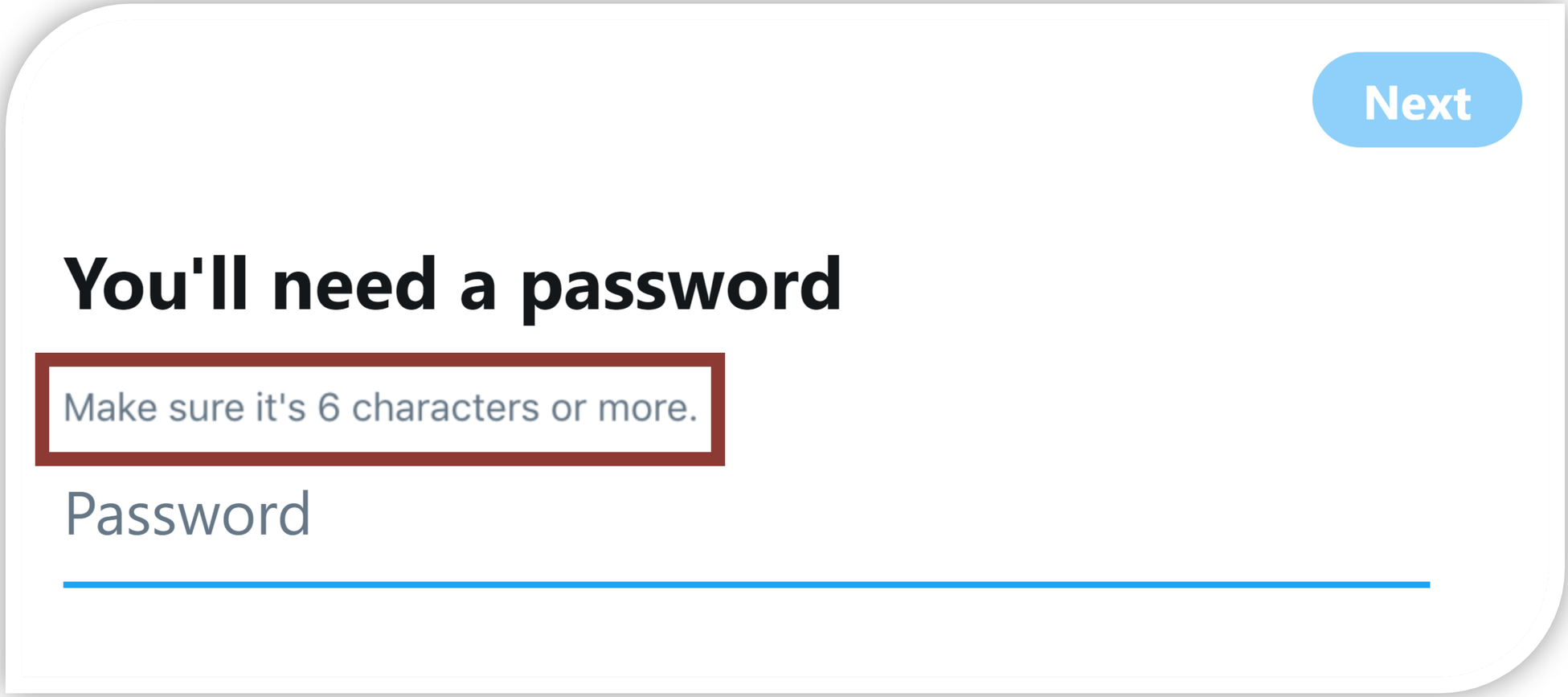
Richard Shay, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Alain Forget, Saranga Komanduri, Michelle L. Mazurek*, William Melicher, Sean M. Segreti, Blase Ur

Carnegie Mellon University
Pittsburgh, PA
{rshay, lbauer, nicolasc, lorrie, aforget, sarangak, billy, ssegreti, bur}@cmu.edu

*University of Maryland
College Park, MD
mmazurek@cs.umd.edu

Password Creation in the Presence of Blacklists

Hana Habib, Jessica Colnago, William Melicher, Blase Ur†, Sean Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Cranor
Carnegie Mellon University
{htq, jcolnago, wmelicher, ssegreti, lbauer, nicolasc, lorrie}@andrew.cmu.edu
†University of Chicago
blase@uchicago.edu


Next
You'll need a password
Make sure it's 6 characters or more.
Password

usability of one password

?

usability of many passwords


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

password reuse everywhere

25

password-protected accounts
[Flôrencio & Herley 2007]

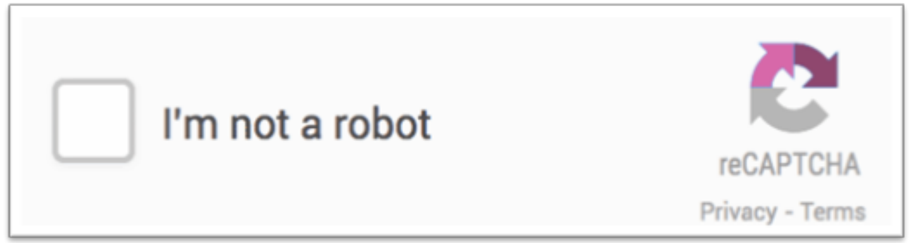
43-51%

of users reuse passwords
[Das et al. 2014]

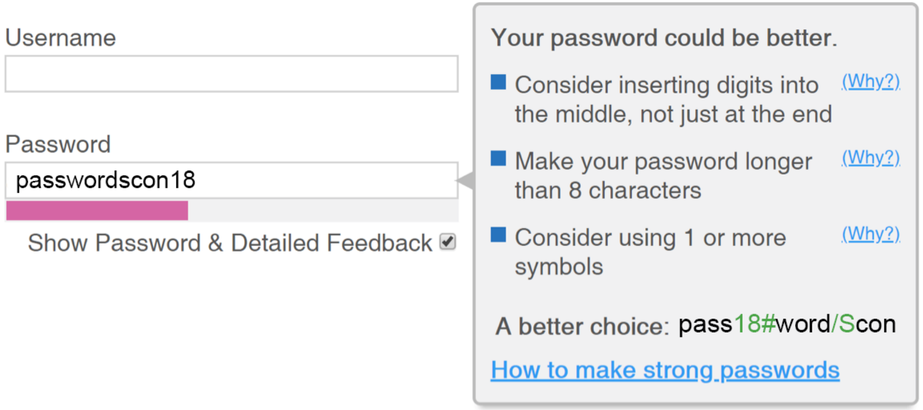
Memory-Hard Hash Function

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

Rate-Limiting Guessing



Password Strength Meter



[IMG: Midge cat by dougwoods on Flickr]

maintaining many passwords = hard


AcmeCo
Email
...
jim@mail.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
...	...




AcmeCo

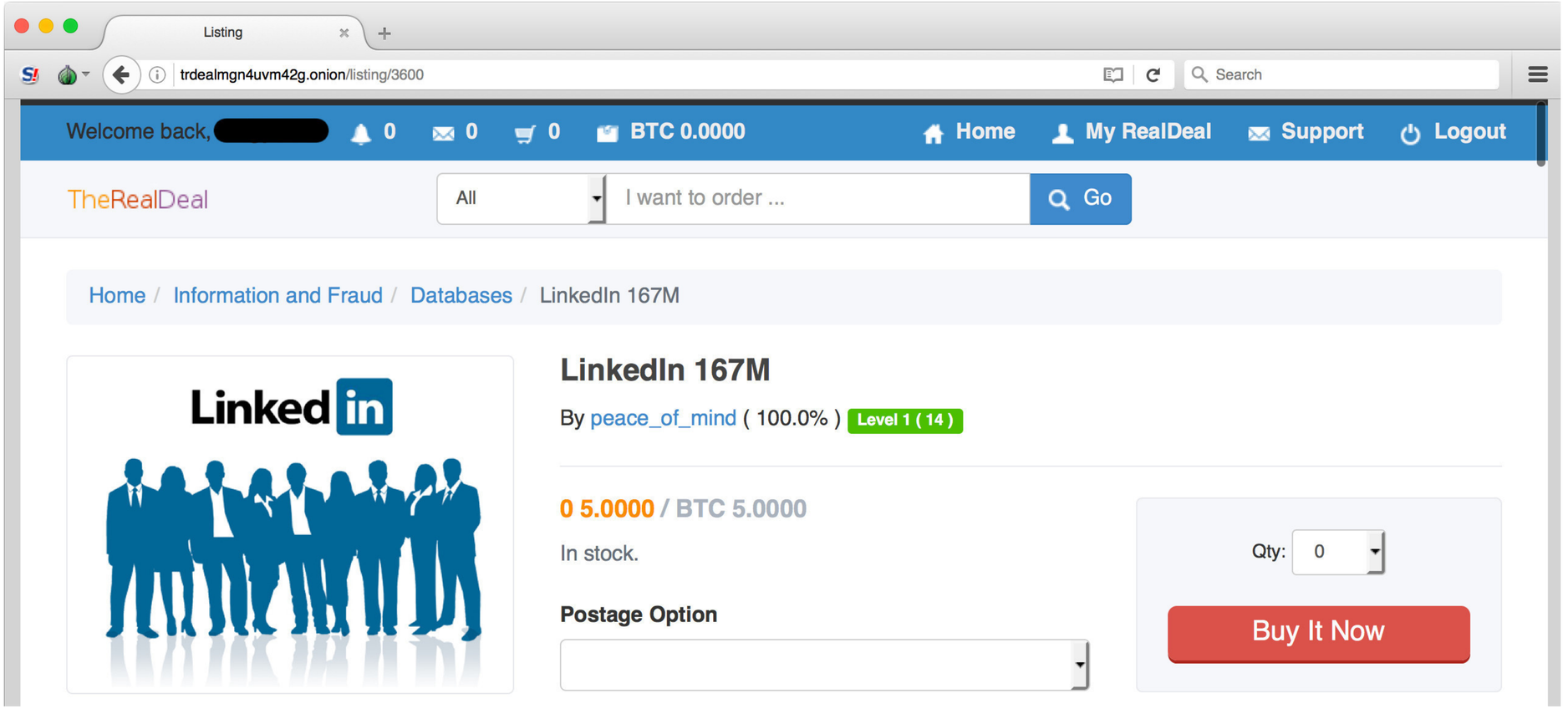
Email	Argon2i Hash of Password
…	…
jim@mail.com	`$argon2i$v=19$m=4096,…`
…	…

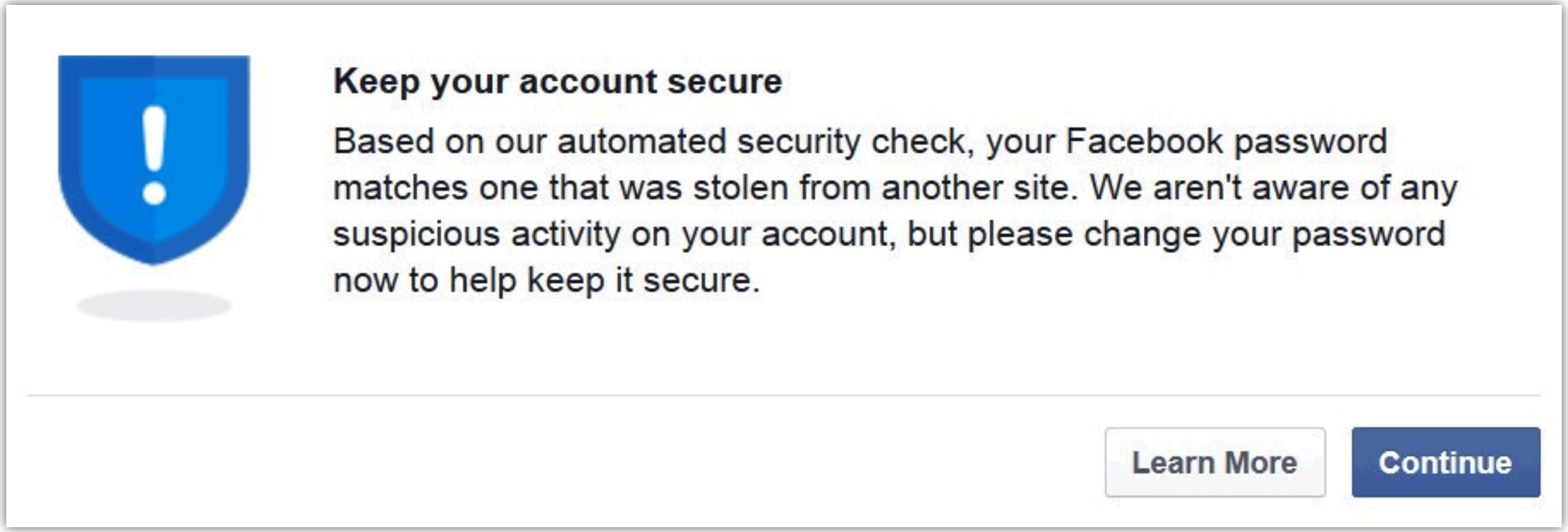
LinkedIn

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

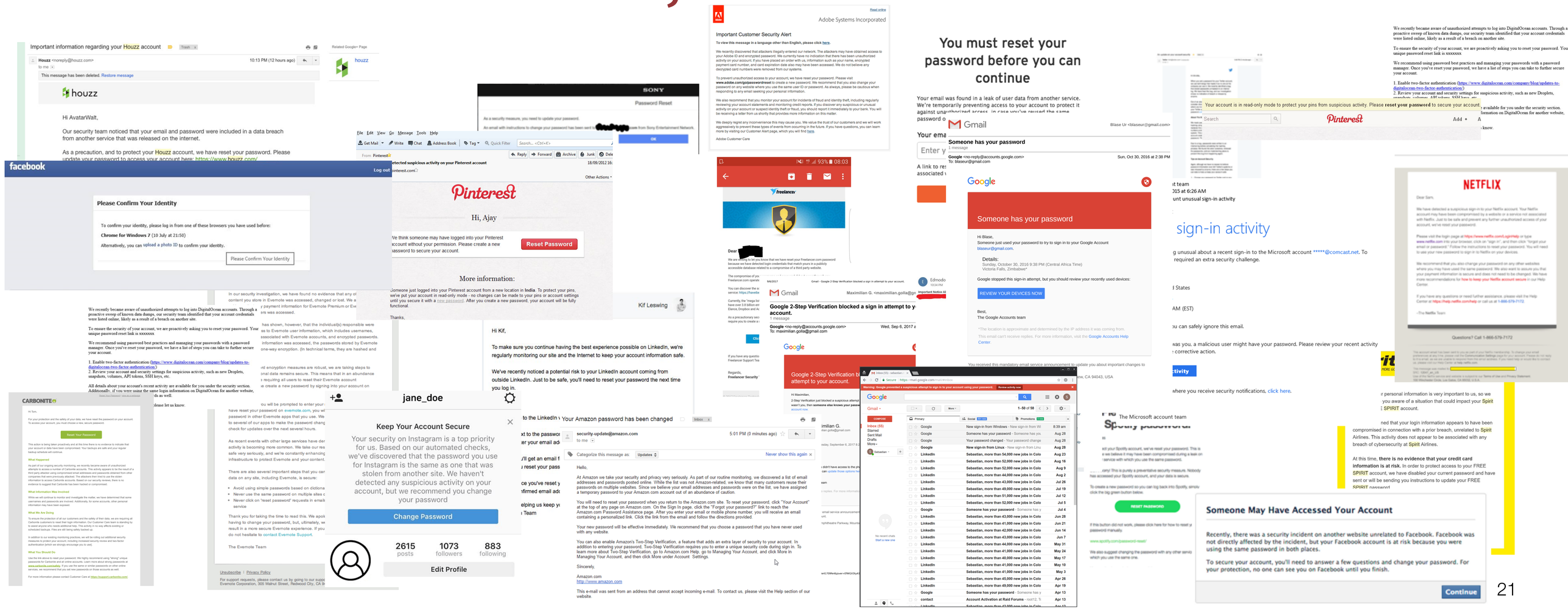
1 guess is enough!

black-market monitoring




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

but wait, there's more



"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
SUPER Security, Usability, & Privacy Education & Research

Toronto, Canada | ACM CCS | October 18, 2018

STUDY 1

previously sent password-reuse notifications

STUDY 2

individual components of password-reuse notifications

6 representative notifications

why did you receive this notification?

60% hacked account

21% data breach

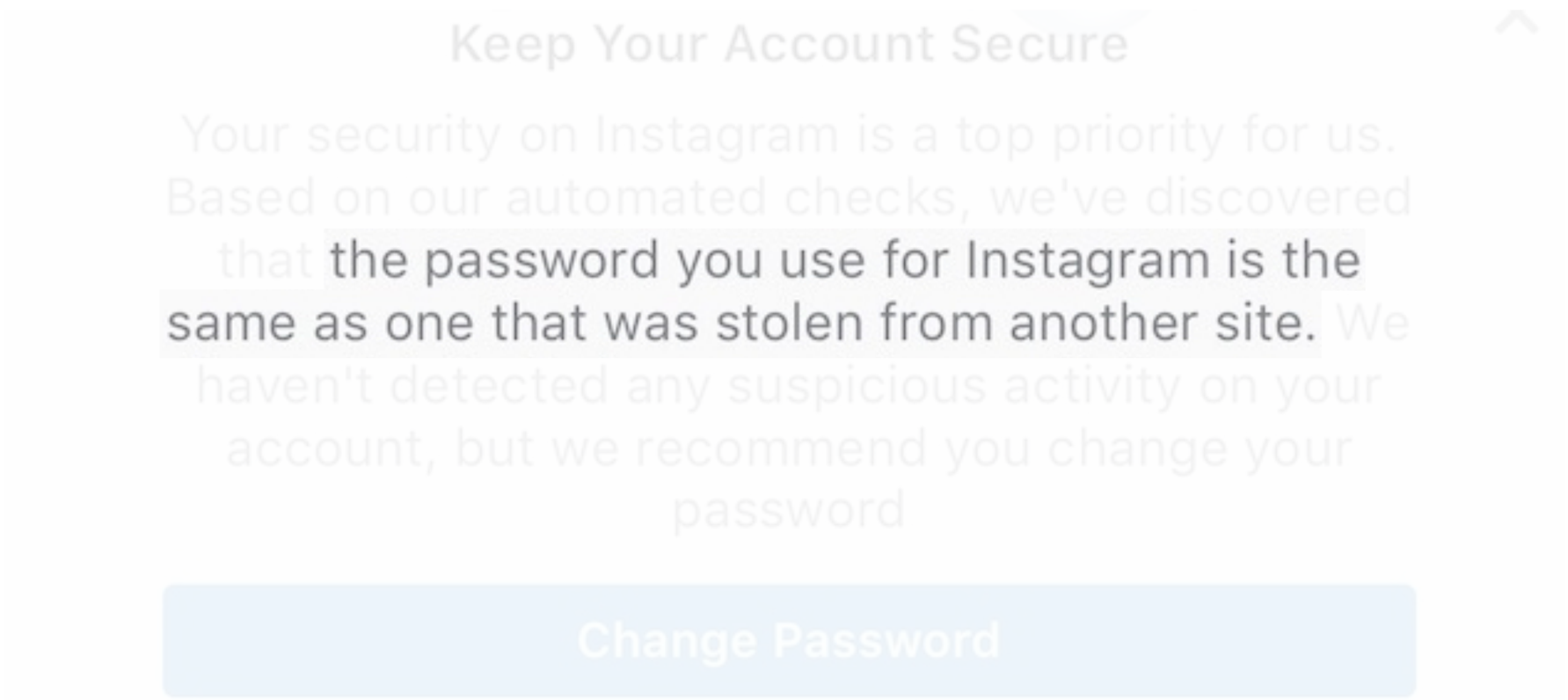
don't mention password reuse

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
Change Password

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

1. lots of people do
2. black markets
3. automation
4. password mangling
5. …

“…guessing that I use ‘password’ as my password…”

1. lots of people do

understanding why password reuse is bad = hard

usability of one password ≠ usability of many passwords

The Password Doesn't Fall Far: How Service Influences Password Choice

Miranda Wei, The University of Chicago
Maximilian Golla, Ruhr University Bochum
Blase Ur, The University of Chicago

Baltimore, USA | August 12, 2018

https://myappletrees.com

Create a password for your MyAppleTrees account:

MyAppleTreesPassword

https://myappletrees.com

Create a password for your MyAppleTrees account:

RedDelicious

five password leaks

yes, related to name

Battlefield (Gaming)		Brazzers (Adult)		Last.fm (Music)		LinkedIn (Social)		Mate1 (Dating)	
Password	Of Total	Password	Of Total	Password	Of Total	Password	Of Total	Password	Of Total
battlefield	0.053 %	brazzers	0.064 %	lastfm	0.150 %	linkedin	0.120 %	sexy	0.053 %
lol123	0.028 %	211211	0.022 %	music	0.063 %	linked	0.019 %	mate1	0.050 %
xbox360	0.028 %	giants	0.019 %	abcdefg123	0.049 %	Linkedin	0.012 %	promise	0.033 %
warhammer	0.017 %	titties	0.019 %	last.fm	0.030 %	linkedin1	0.011 %	love123	0.024 %
starwars1	0.016 %	bigboobs	0.018 %	foxpass	0.025 %	zzzzzzzz	0.011 %	looking	0.023 %
runescape	0.015 %	pornstar	0.017 %	musica	0.024 %	krishna	0.010 %	olamide	0.017 %
fp2241	0.014 %	patriots	0.013 %	qqww1122	0.013 %	sairam	0.009 %	money6	0.016 %
4815162342	0.014 %	braves	0.012 %	ahov	0.011 %	super123	0.009 %	kissme	0.015 %
bfheroes	0.013 %	iverson	0.011 %	A123456	0.009 %	linkedin123	0.008 %	damilola	0.015 %
hejsan	0.012 %	hooters	0.011 %	ahovwpib	0.009 %	LinkedIn	0.008 %	lovingyou	0.015 %

Top ten passwords per service after filtering

yes, related to topic

trooper

headshot

iamthebest

pornstar

enjoyporn

iloveporn

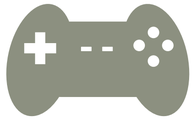
networking

jobsearch

business

based on other interests

halflife



warcraft3

gamecube

viewsonic

giants

patriots

wrestling

bowling

cadillac

silverado

peterbilt

accord

reflect international backgrounds

`hejhej`

`jemoeder`

`wachtwoord`

`panzer`

`olamide`

`opeyemi`

`babatunde`

`adekunle`

users invoke religion when it comes to jobs and love

krishna	ilovegod
jesuschrist	thankgod
godisgreat	ingodwetrust
godislove	godhelpme

coming up with unique passwords = hard

conclusion

there are key usability challenges unique to password reuse


ZOHO


1Password


LastPass


dashlane


True Key


Google


twitter


Dropbox


LinkedIn


Microsoft

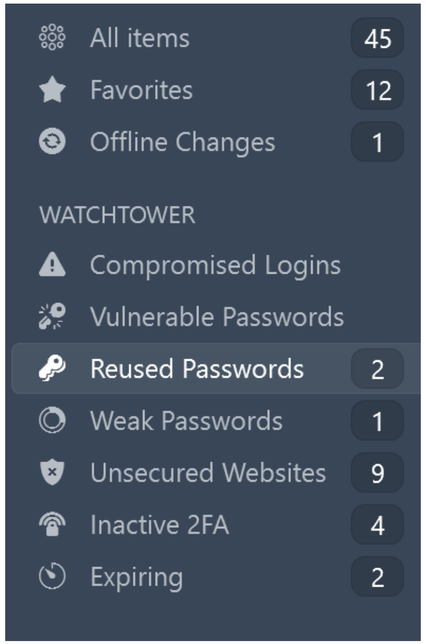

AcmeCo

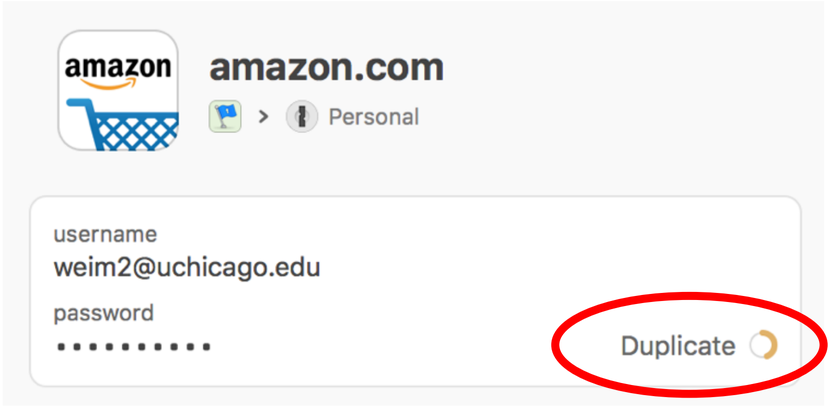

SONY


reddit

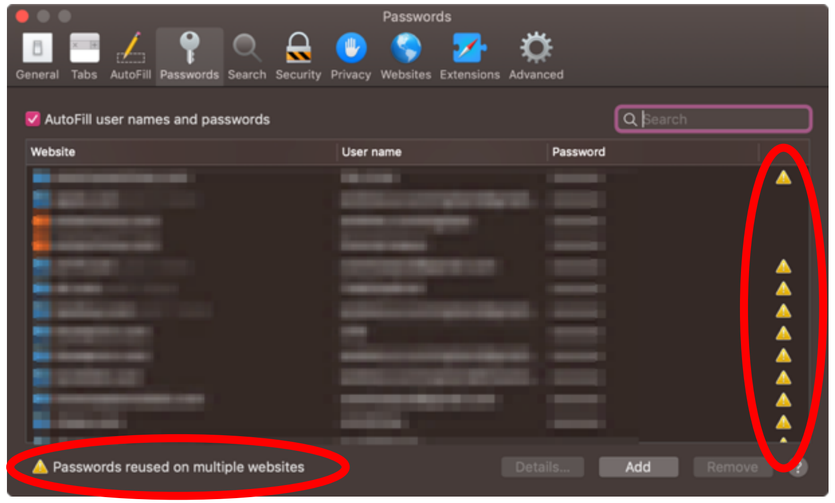

ebay


facebook





1Password

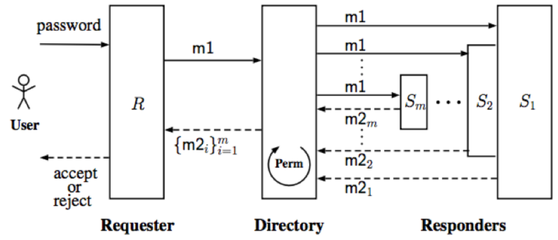


macOS Mojave, Safari 12

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



Everything but the User: Reducing Password Reuse

Miranda Wei, The University of Chicago

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