14. Authentication
Part 2

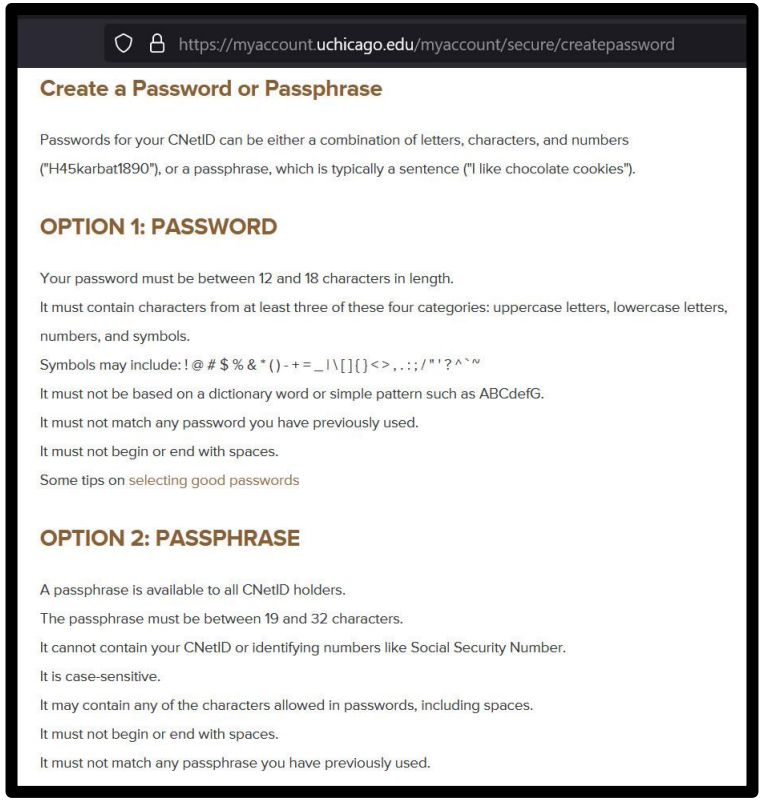
Blase Ur and Grant Ho
February 21st, 2024
CMSC 23200

THE UNIVERSITY OF CHICAGO

How Do We Help Users Make Better Passwords?

Password-Composition Rules

- Goal: Increase the password space
- In practice, many users comply in predictable ways



Password Expiration

- Goal: Make sure stolen passwords are invalid by the time the attacker cracks them
- Require password change every X days? (No!)

Problem 1: Bad Advice

Carnegie Mellon University

Password Requirements

Must Contain

- At least 8-characters.
- At least one uppercase alphabetic character (e.g., A-Z).
- At least one lowercase alphabetic character (e.g., a-z).
- At least one number (e.g., 0-9).
- At least one special character (e.g., []~!@#$%^&*()?<>./_-+=).

Cannot Contain

- Known information (i.e., first name, last name, Andrew userID, date of birth, 9-digit Carnegie Mellon ID number, SSN, job title).
- Four or more occurrences of the same character (e.g., aaaa, 2222, a123a345a678a).*
- A word that is found in a standard dictionary.* (after removing non-alpha characters).

****This requirement does not apply to Andrew account passwords that are more than 19 characters in length (e.g., passphrase).***

Additional Policies

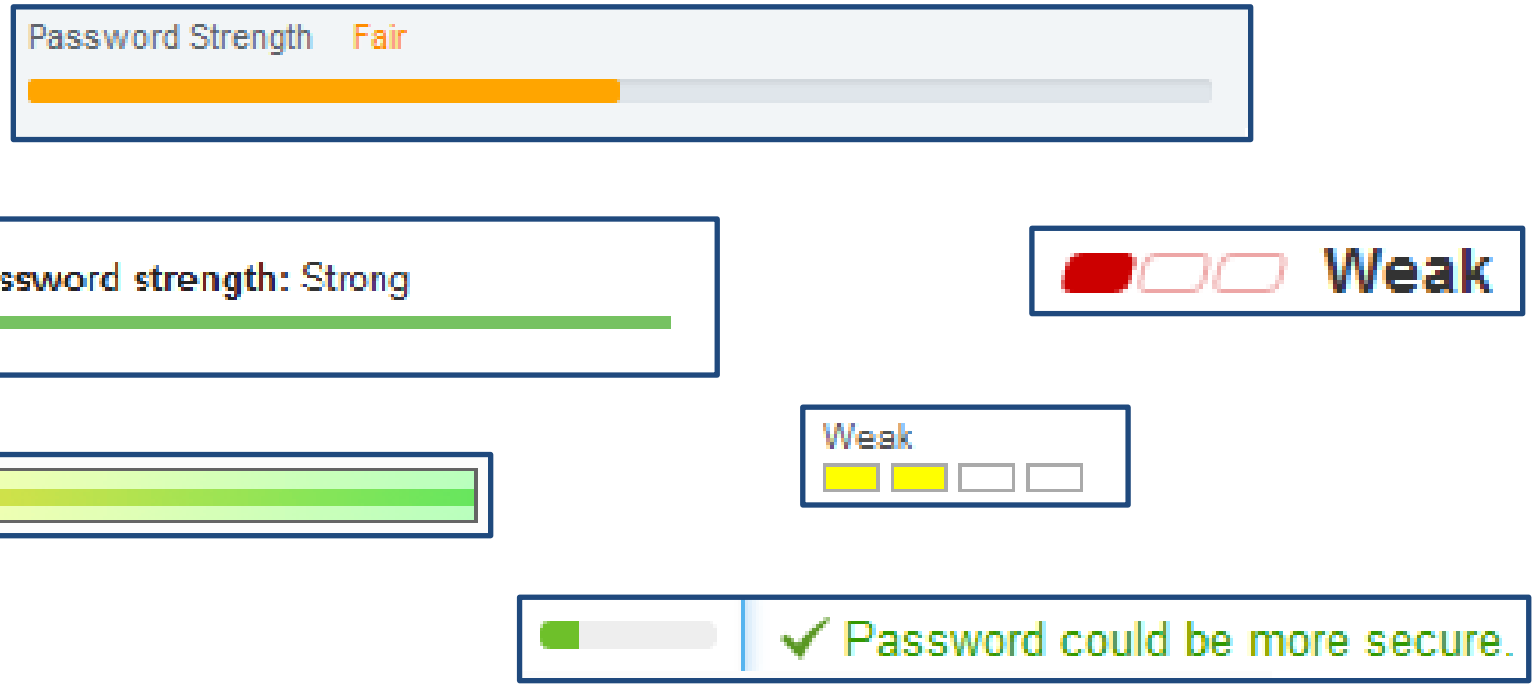
- Last five passwords cannot be used.
- Cannot be changed more than four times in a day.

Problem 2: Inaccurate Feedback

Problem 3: Unhelpful Feedback

Proactive Strength Checking

- Initial idea: provide feedback
- In practice: complexities regarding what to model, and how to do so efficiently



User-Centered Security

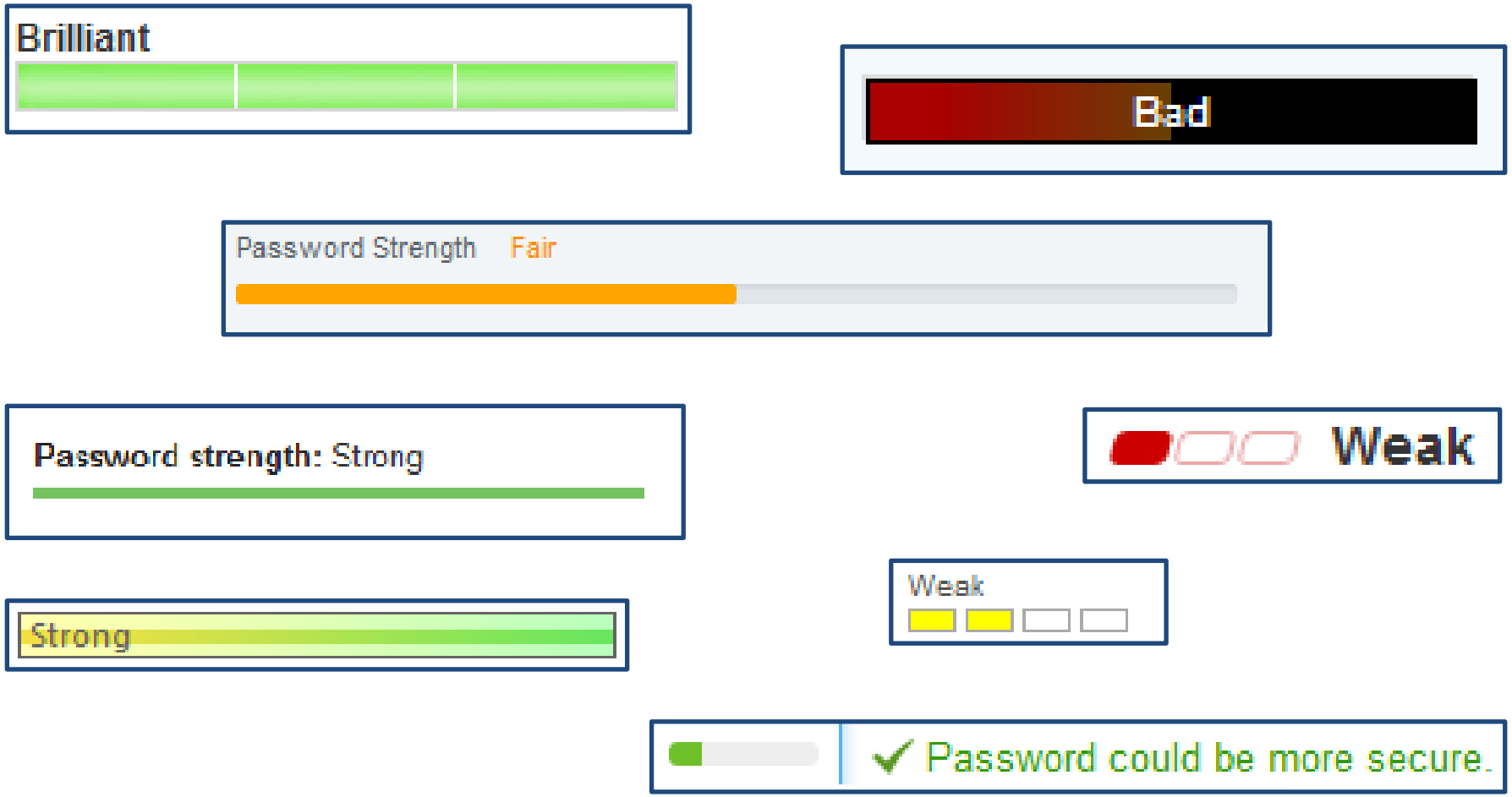
Some Ways to Understand Users

- Retrospective analysis of password breaches
- Large-scale online studies
- Examine real passwords with permission
- Qualitative studies

Meters' Security & Usability Impact

Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *Proc. USENIX Security Symposium*, 2012.

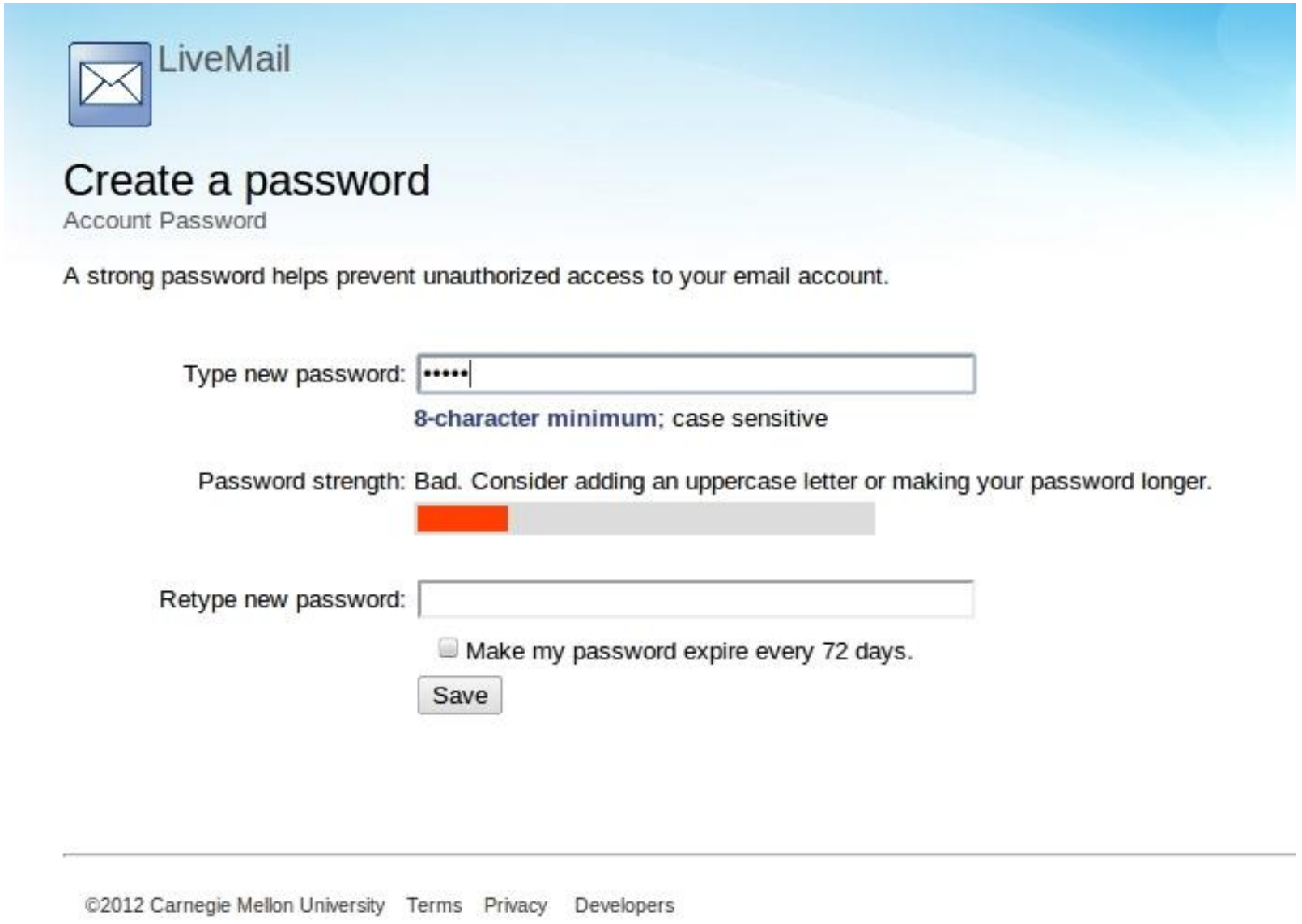
Meters Are Ubiquitous



Test Meters' Impact

- How do meters impact password security?
- How do meters impact usability?
  - Memorability
  - User sentiment
  - Timing
- What meter features matter?
- 2,931-participant online study

Baseline Password Meter



Visual Differences

Type new password: usenIX

8-character minimum; case sensitive

Baseline meter

Fair. Consider adding a digit or making your password longer.

Three-segment

Fair. Consider adding a digit or making your password longer.

Green

Fair. Consider adding a digit or making your password longer.

Tiny

Fair. Consider adding a digit or making your password longer.

Huge

Fair. Consider adding a digit or making your password longer.

No suggestions

Fair.

Text-only

Fair. Consider adding a digit or making your password longer.

Visual Differences

Type new password: usenIX

8-character minimum; case sensitive

Baseline meter

Fair. Consider adding a digit or making your password longer.

Three-segment

Fair. Consider adding a digit or making your password longer.

Green

Fair. Consider adding a digit or making your password longer.

Tiny

Fair. Consider adding a digit or making your password longer.

Huge

Fair. Consider adding a digit or making your password longer.

No suggestions

Fair.

Text-only

Fair. Consider adding a digit or making your password longer.

Scoring Differences

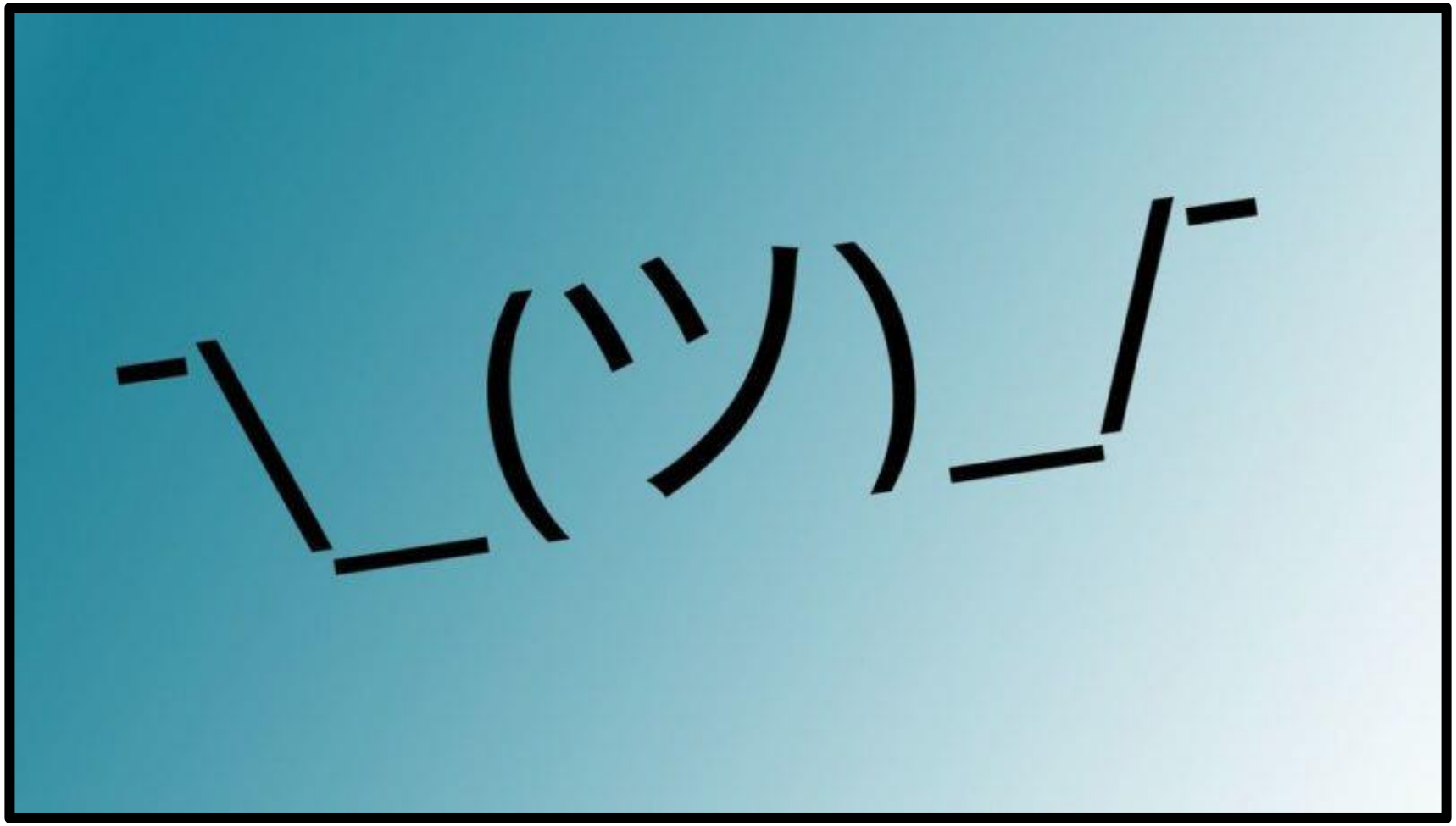
Key Results

- Stringent meters with visual bars increased resistance to guessing
- Visual differences did not significantly impact resistance to guessing
- No significant impact on memorability

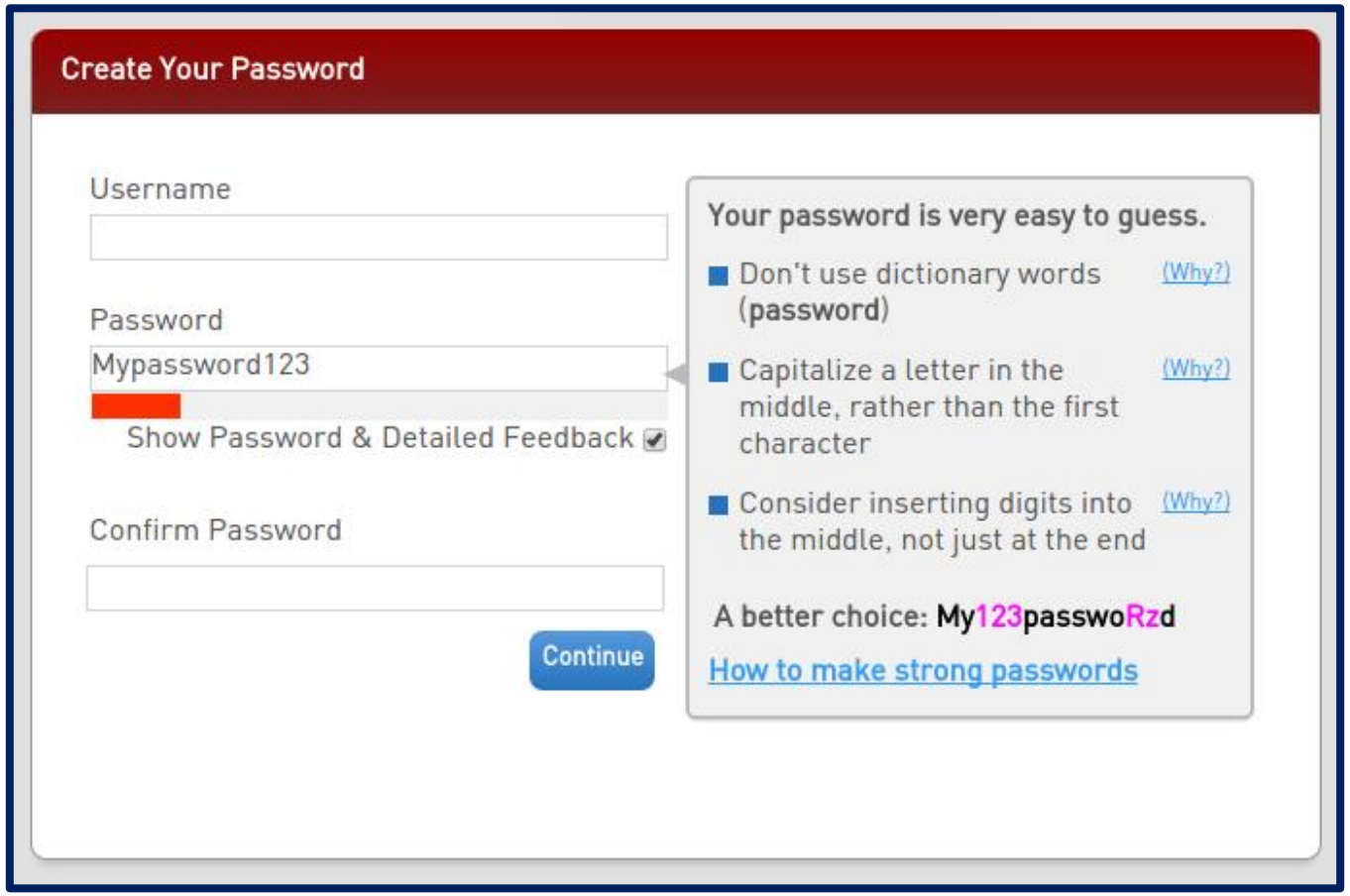
(Revisiting) RNN Password Model Key Results

- Neural networks produce better guesses than previous methods
- Larger model not a major advantage
- Browser implementation in JavaScript

Intelligibility (Explanations)



Building a Data-Driven Meter



Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, Noah Johnson, William Melicher. Development and Evaluation of a Data-Driven Password Meter. In *Proc. CHI*, 2017.

We designed & tested a meter with:

1) Principled strength estimates (RNN)

2) Data-driven feedback to users

We designed & tested a meter with:

1) Principled strength estimates (RNN)

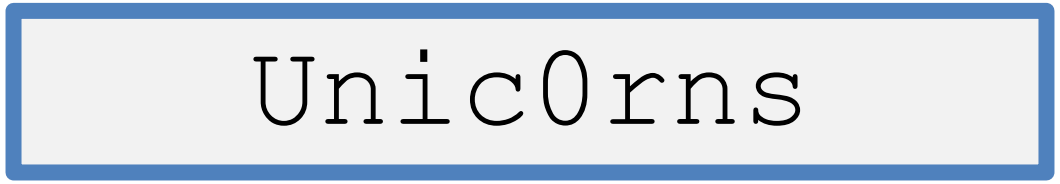
2) Data-driven feedback to users

We designed & tested a meter with:

1) Principled strength estimates (RNN)

2) Data-driven feedback to users

Provide Intelligible Explanations

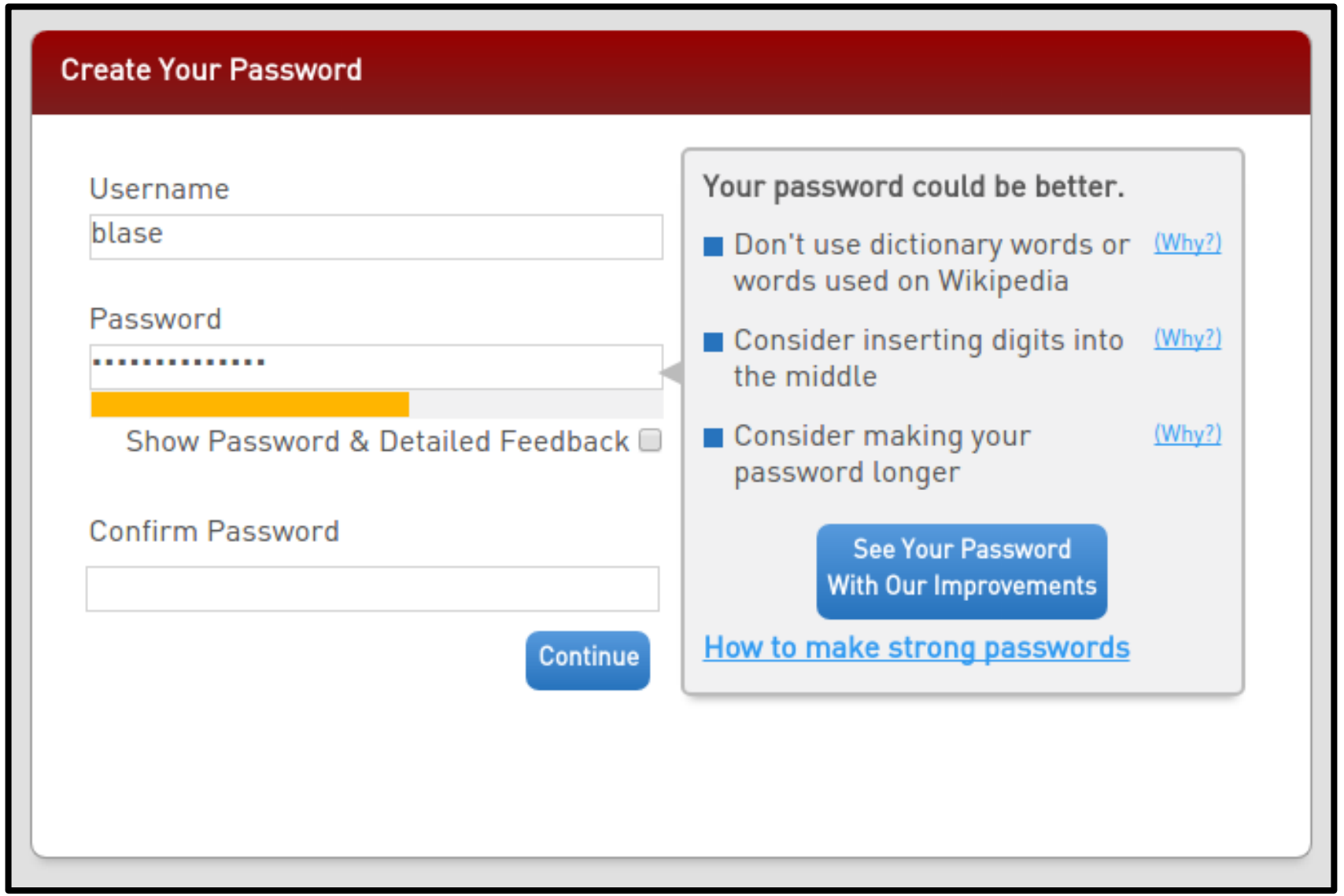


Don't use simple transformations of words or phrases (**unicorns** → **Unic0rns**)

Capitalize a letter in the middle, rather than the first character

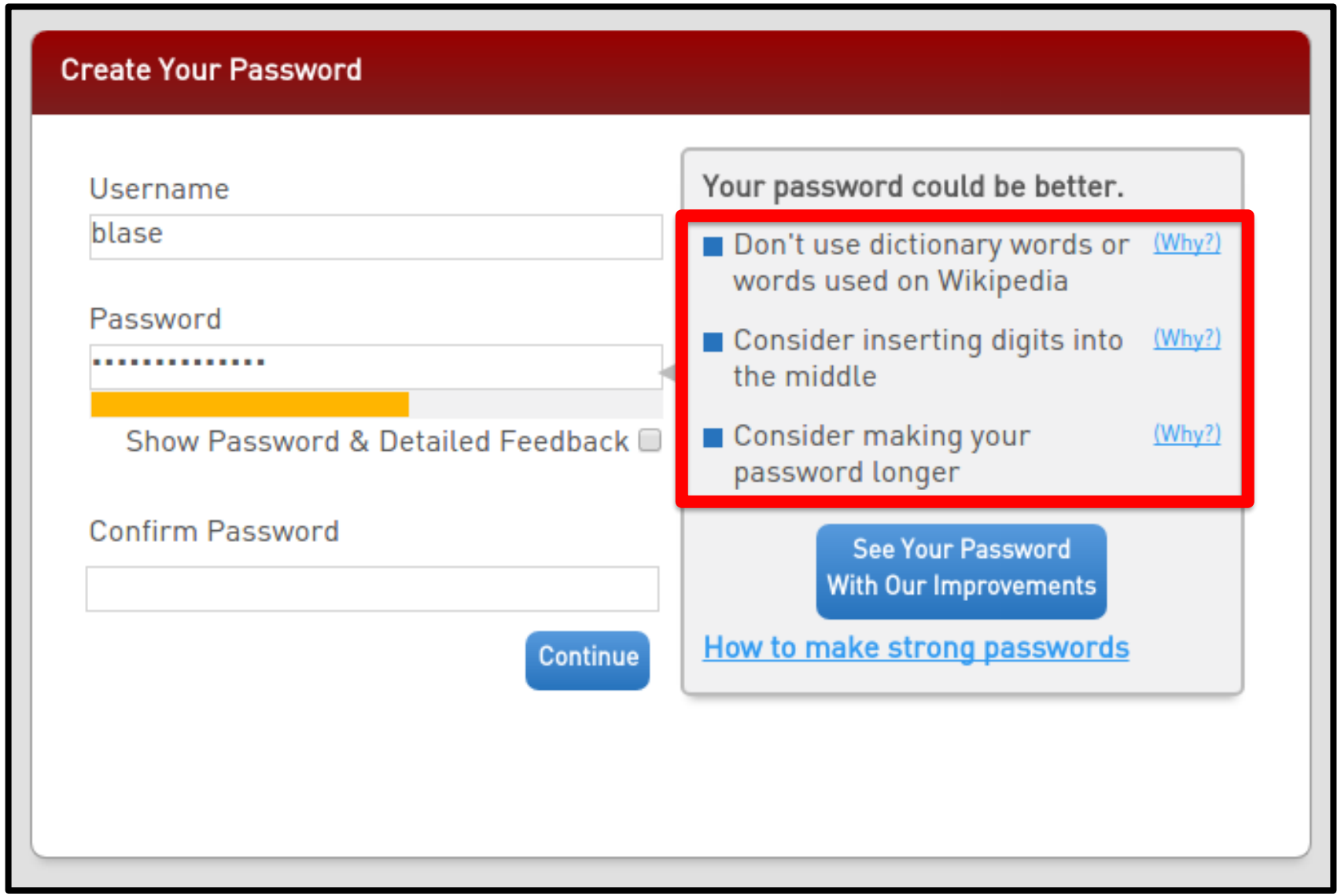
- 21 characteristics
- Weightings determined with regression

After Requirements Are Met…

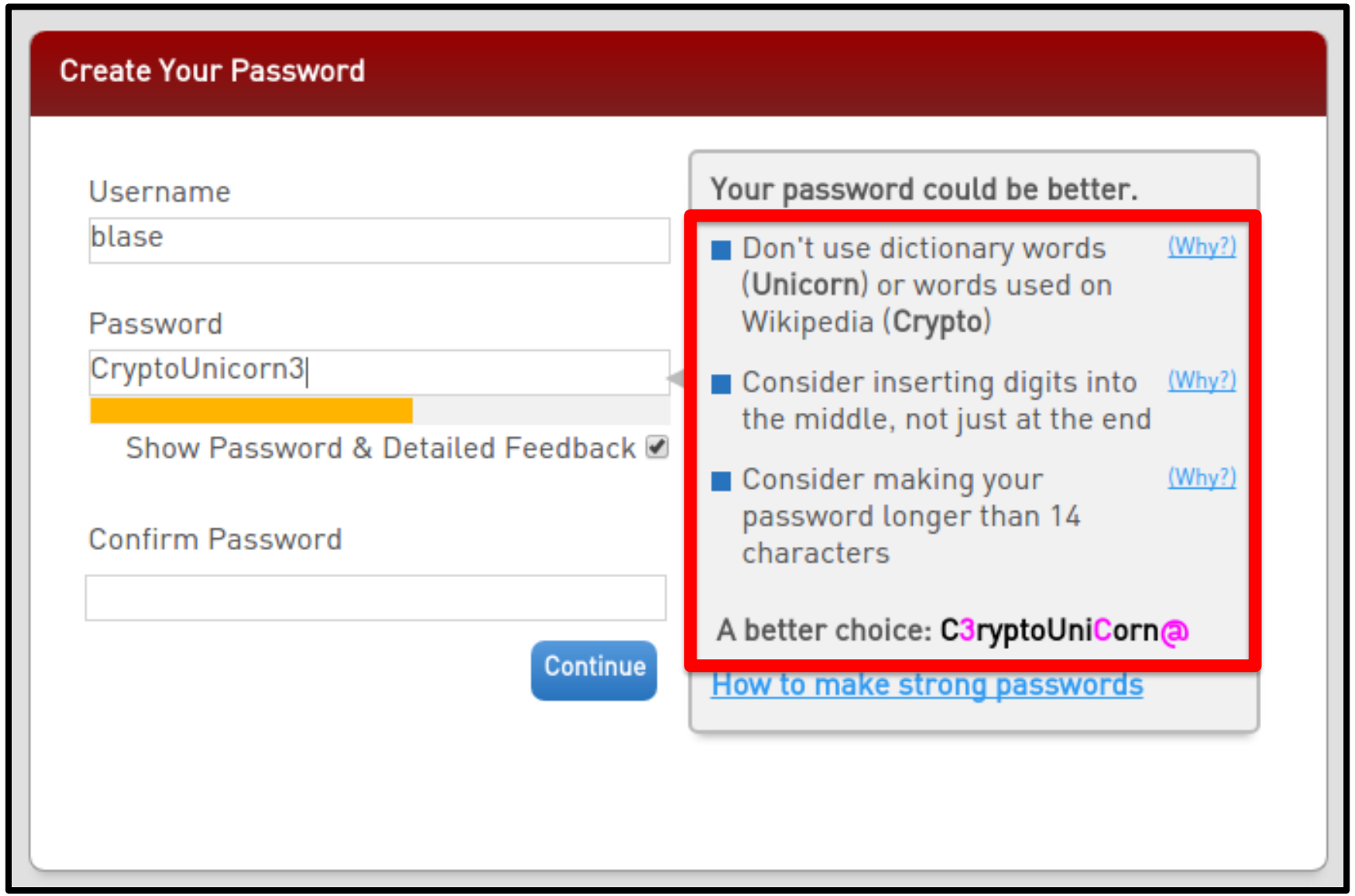


…Displays Score Visually

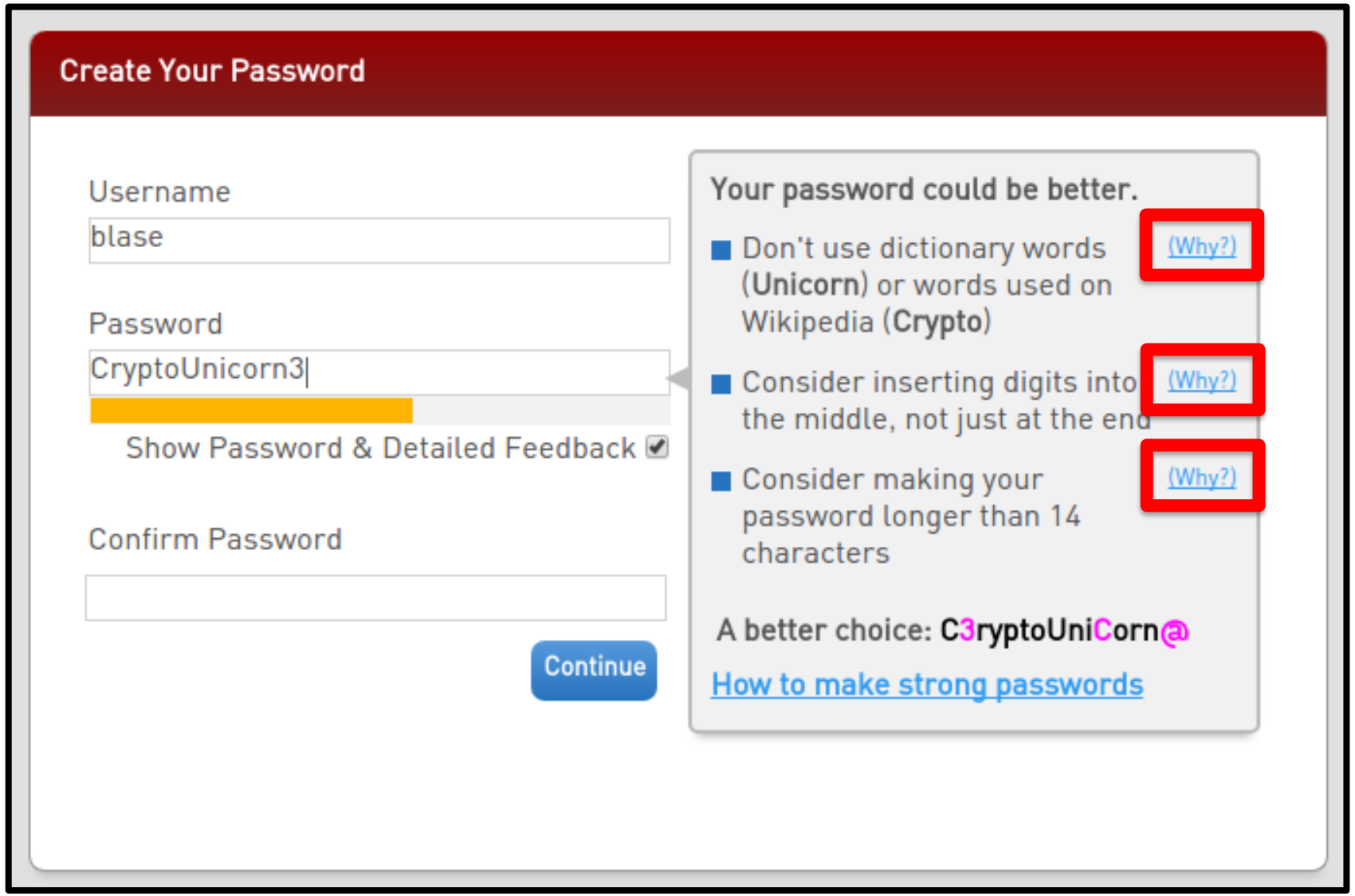
…Provides Text Feedback



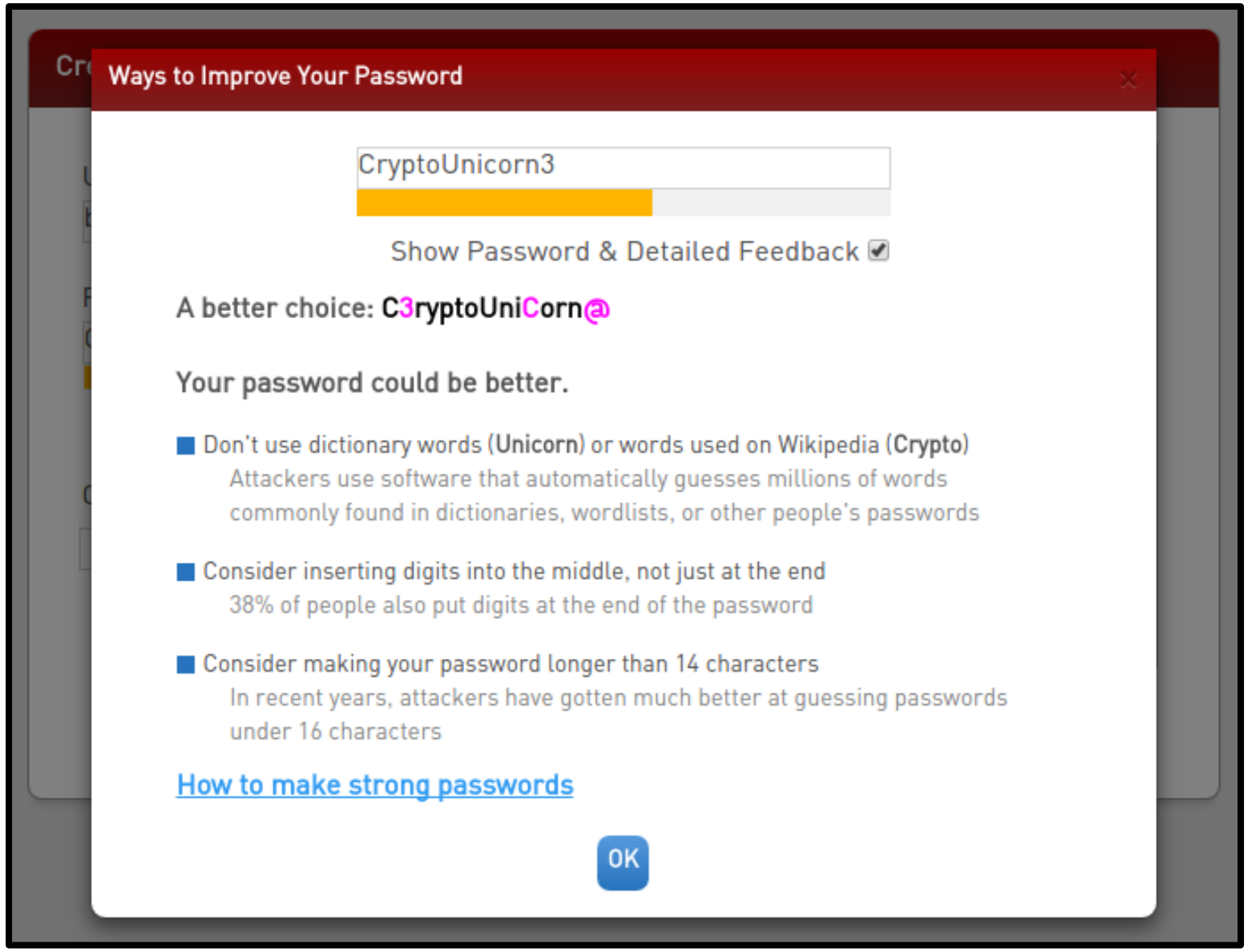
…Gives Detail (Password Shown)



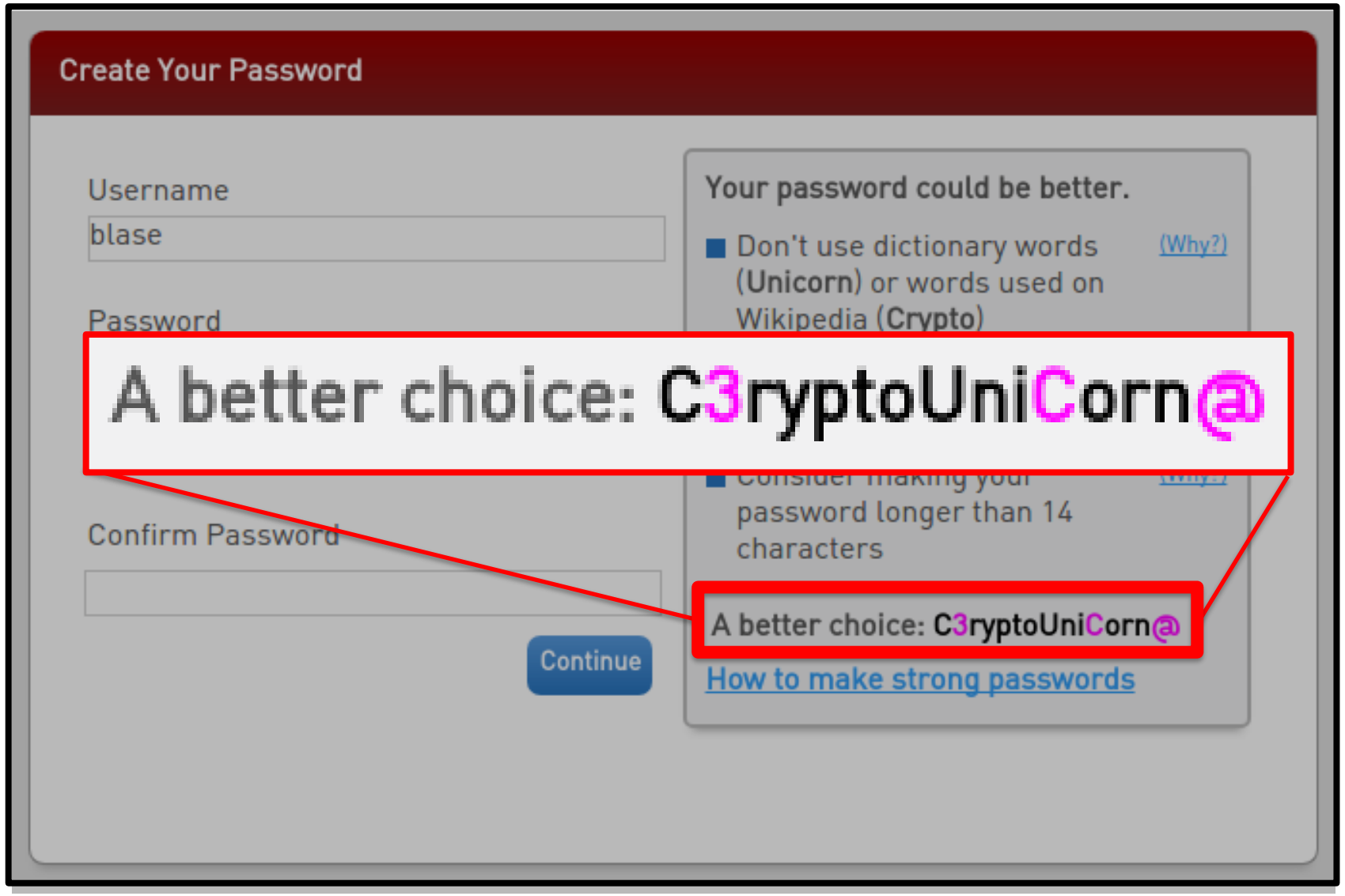
…Offers Explanations



Explanations Shown in Modal

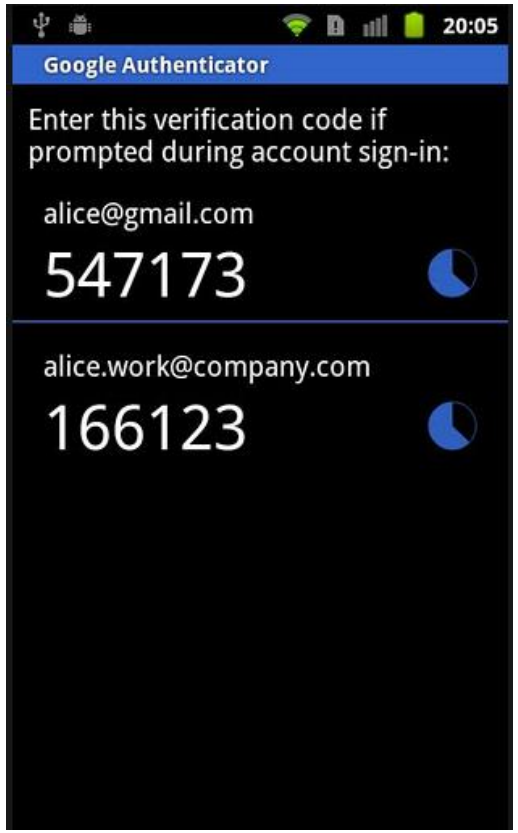


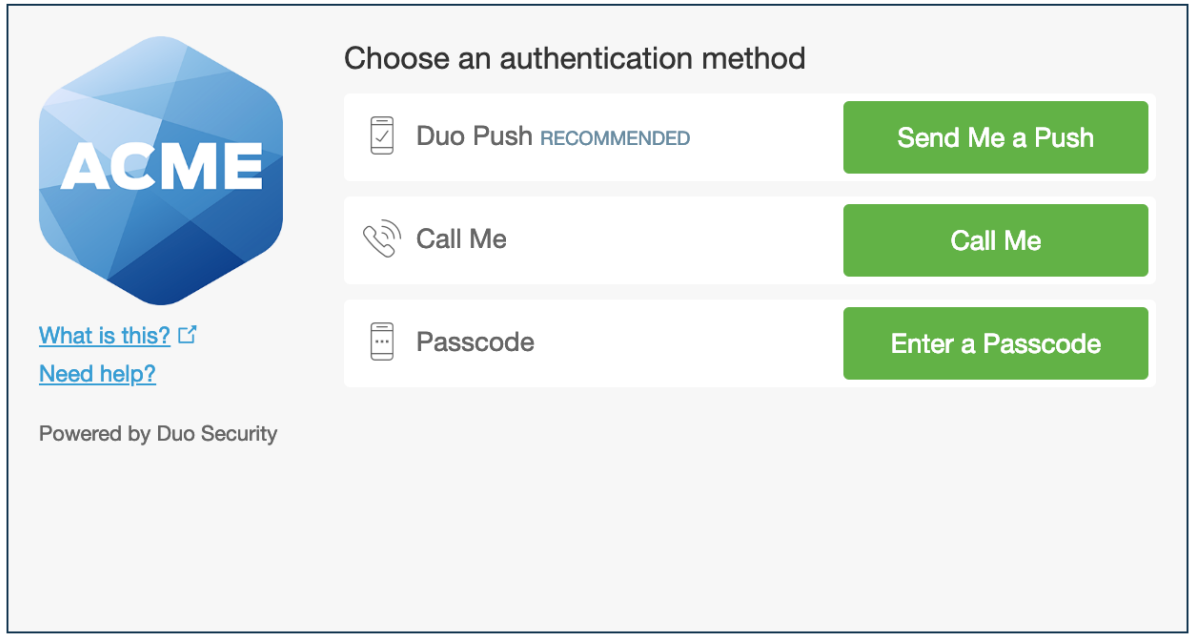
Standard Feedback



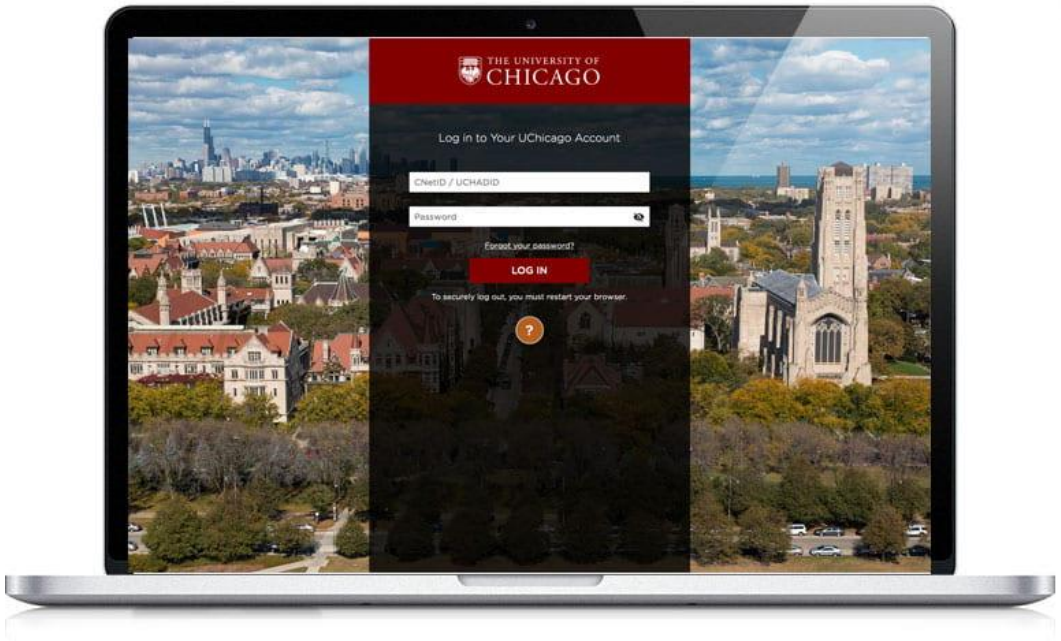
Authentication in Practice: Password Add-Ons / Alternatives

Two-Factor Auth





Single Sign-On



Single Sign-On: Shibboleth

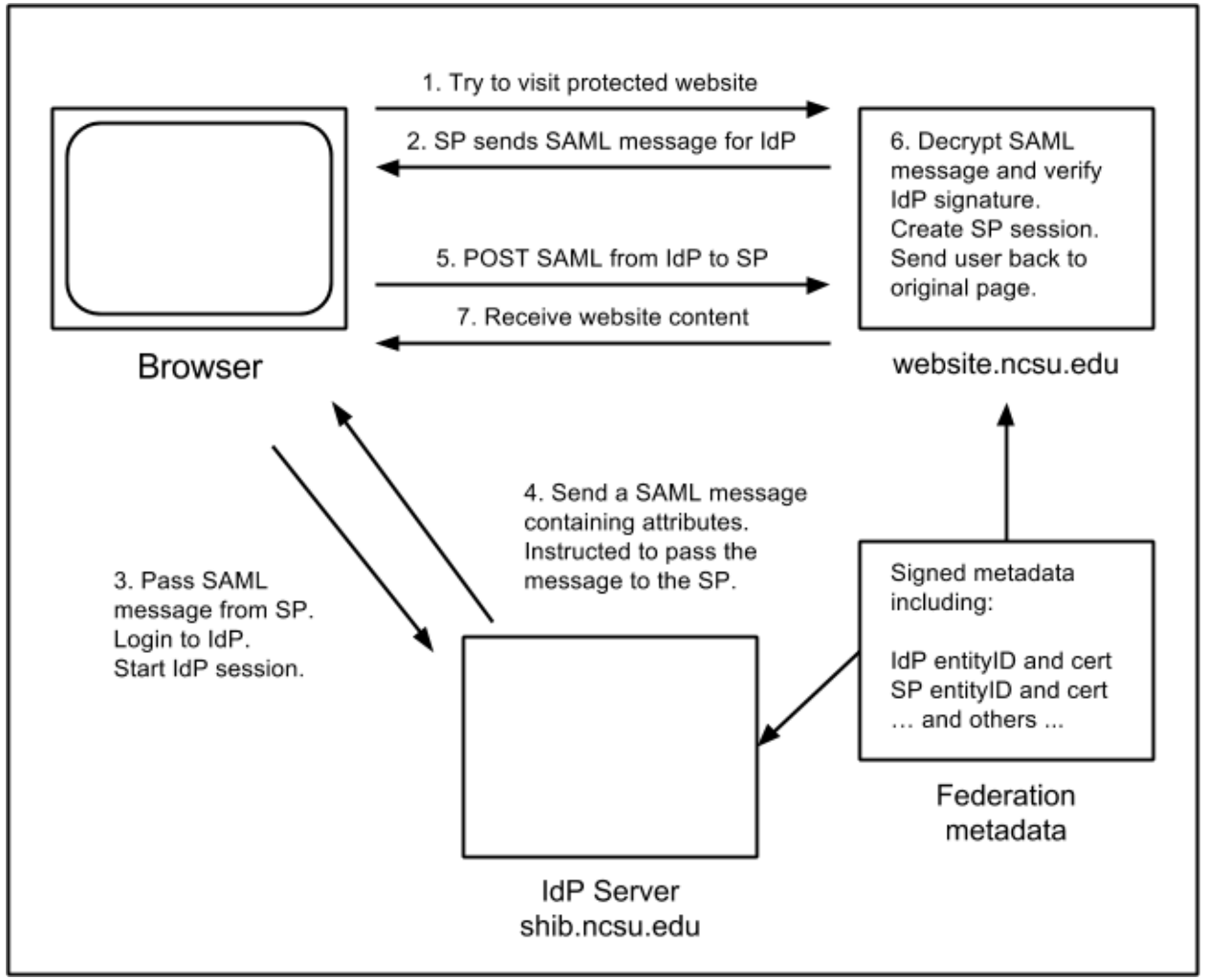


Diagram from https://docs.shib.ncsu.edu/docs/shibworks.html
For a good (long) explanation, see: https://www.switch.ch/aai/demo/

Physical Tokens / Smart Cards

- Codes based on a cryptographic key
  - Token manufacturer also knows the key
- What if there is a breach?

Authentication in Practice: I Forgot My Password

Resetting Accounts

- I forgot my password!
- Send an email?
- Security questions?
- In-person verification?
- Other steps?
- (No backup)

Authentication in Practice: Password Managers

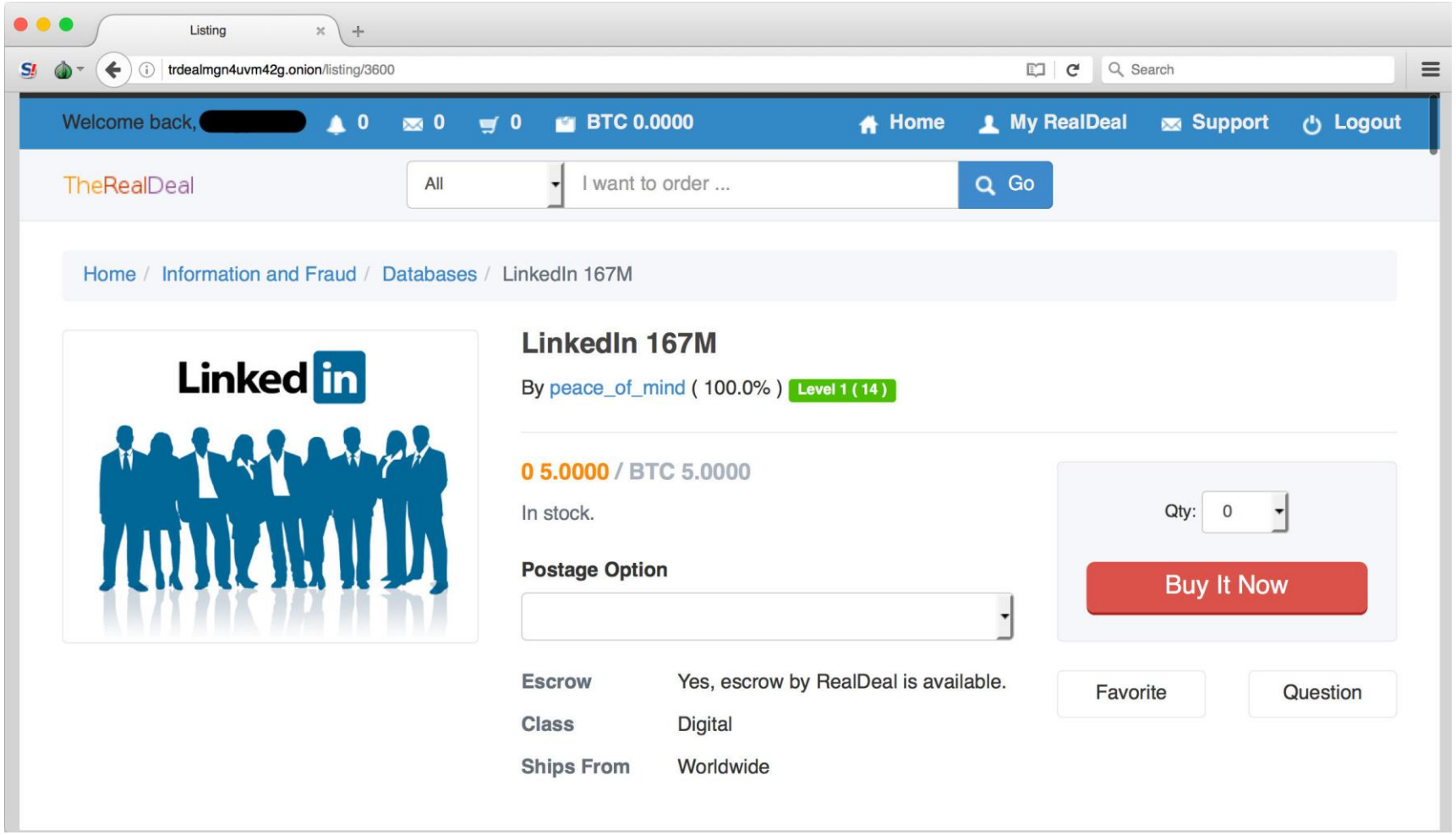
Password Managers

- Trust all passwords to a single master password (still a good idea in most cases)
  - Also trust software
  - Centralized vs. decentralized architectures

1Password

Authentication in Practice: Password Reuse ☹

Monitoring the Black Market



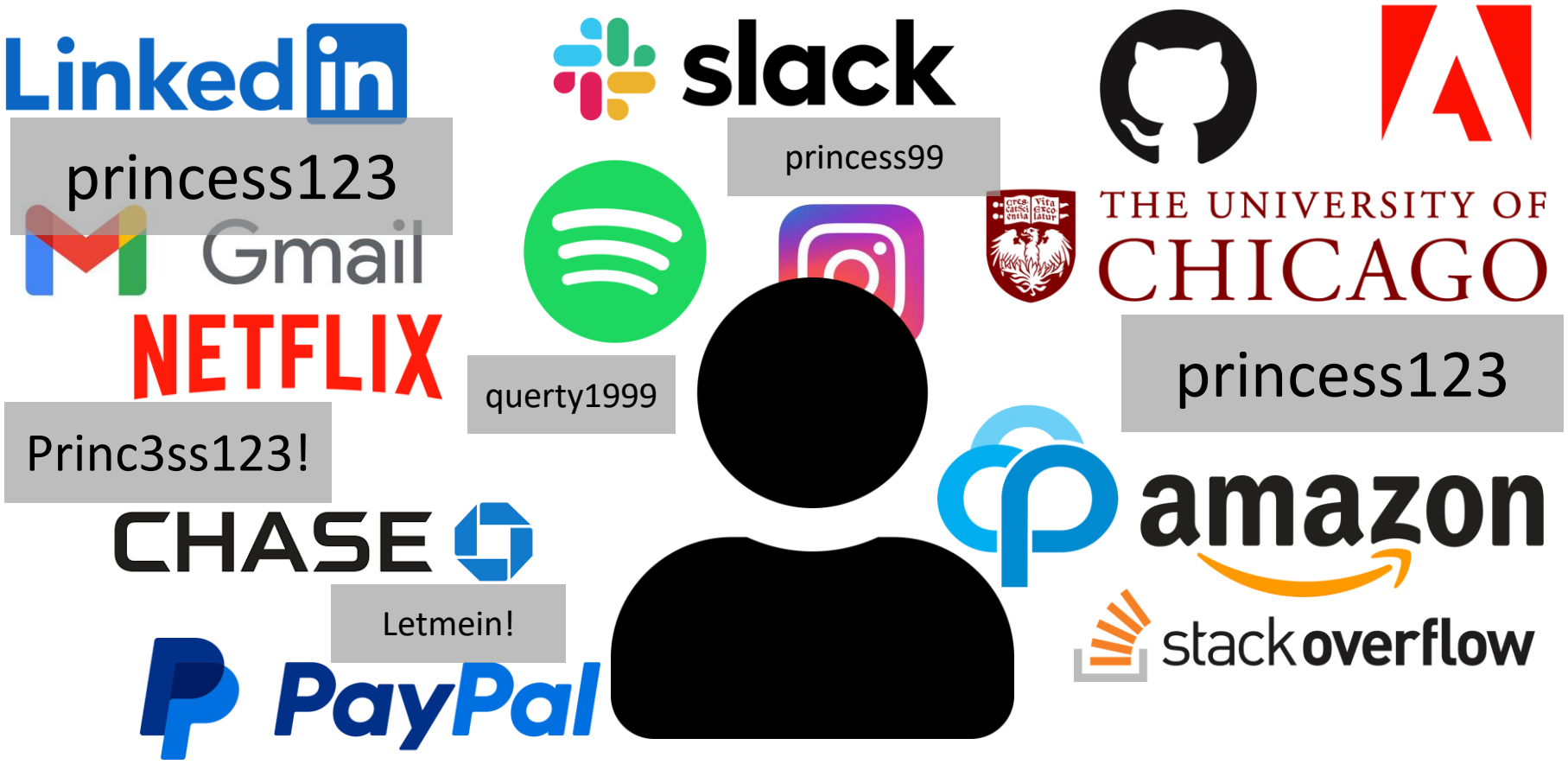
SECURITY

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.

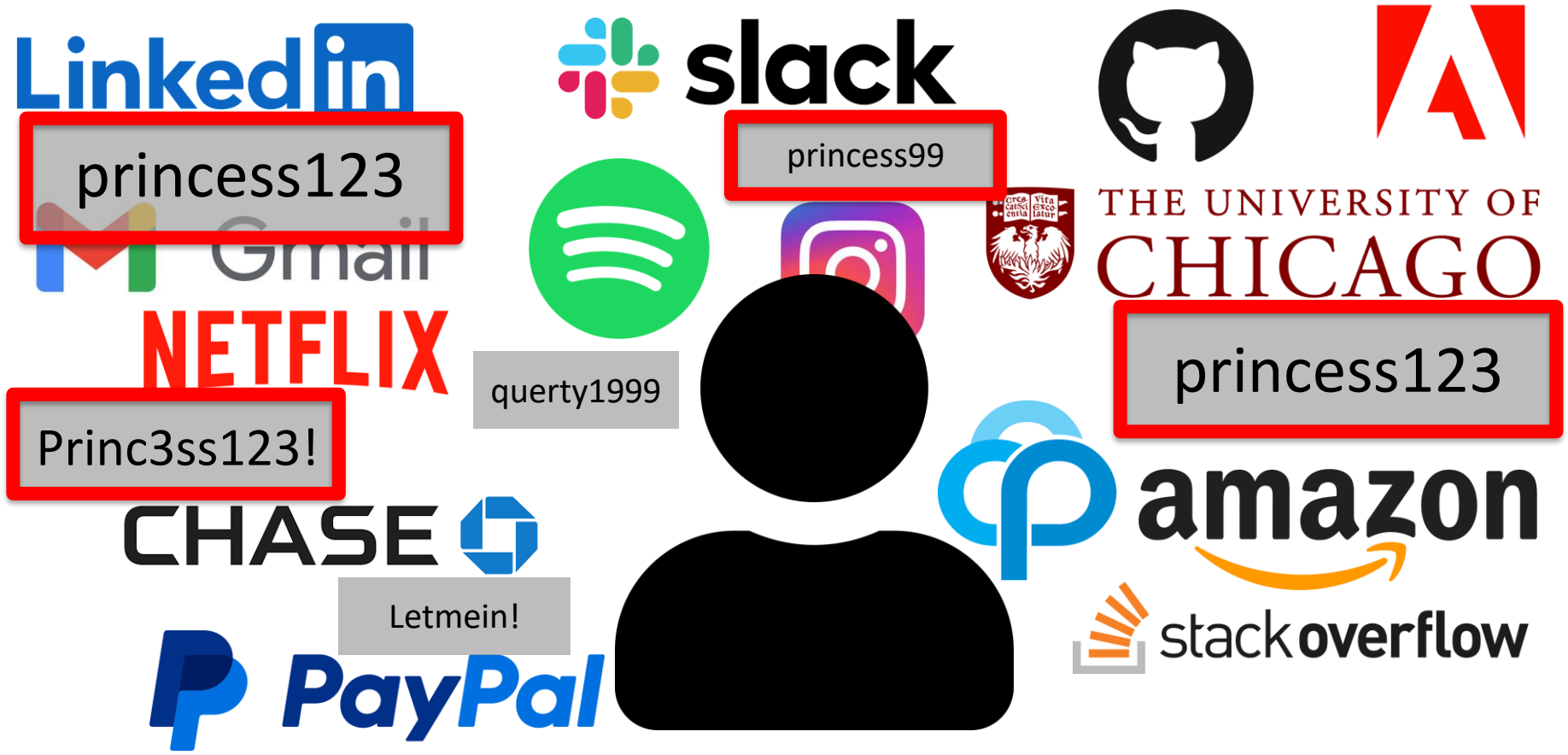
BY KATIE COLLINS | NOVEMBER 9, 2016 12:56 PM PST

Measuring Vulnerability to Password Reuse



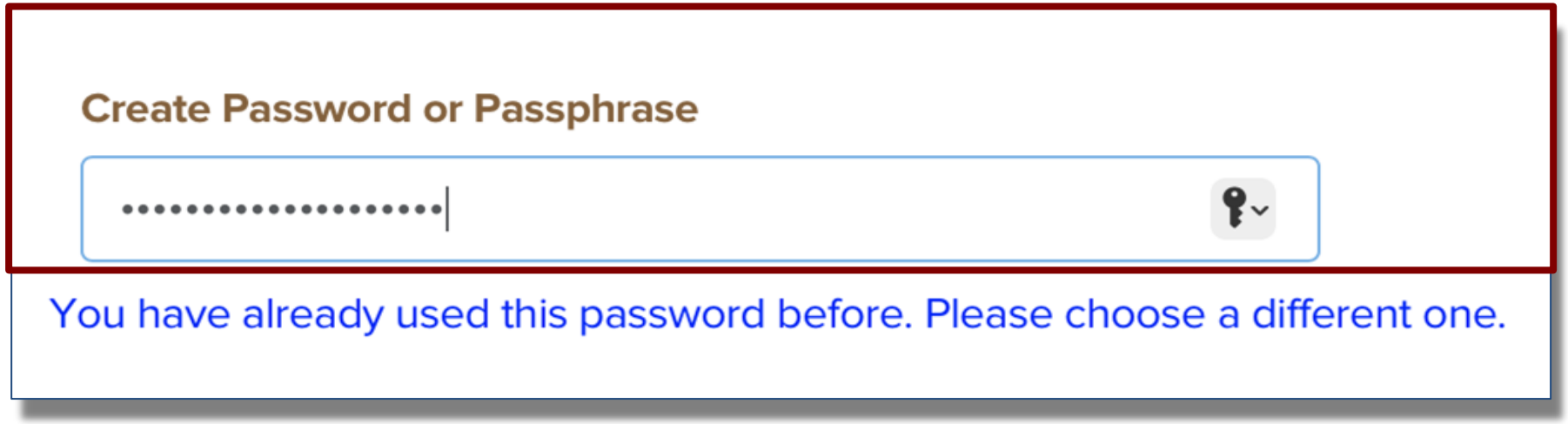
Alexandra Nisenoff, Maximilian Golla, Miranda Wei, Juliette Hainline, Hayley Szymanek, Annika Braun, Annika Hildebrandt, Blair Christensen, David Langenberg, Blase Ur. A Two-Decade Retrospective Analysis of a University's Vulnerability to Attacks Exploiting Reused Passwords. In *Proc. USENIX Security Symposium*, 2023.

Measuring Vulnerability to Password Reuse



Alexandra Nisenoff, Maximilian Golla, Miranda Wei, Juliette Hainline, Hayley Szymanek, Annika Braun, Annika Hildebrandt, Blair Christensen, David Langenberg, Blase Ur. A Two-Decade Retrospective Analysis of a University's Vulnerability to Attacks Exploiting Reused Passwords. In *Proc. USENIX Security Symposium*, 2023.

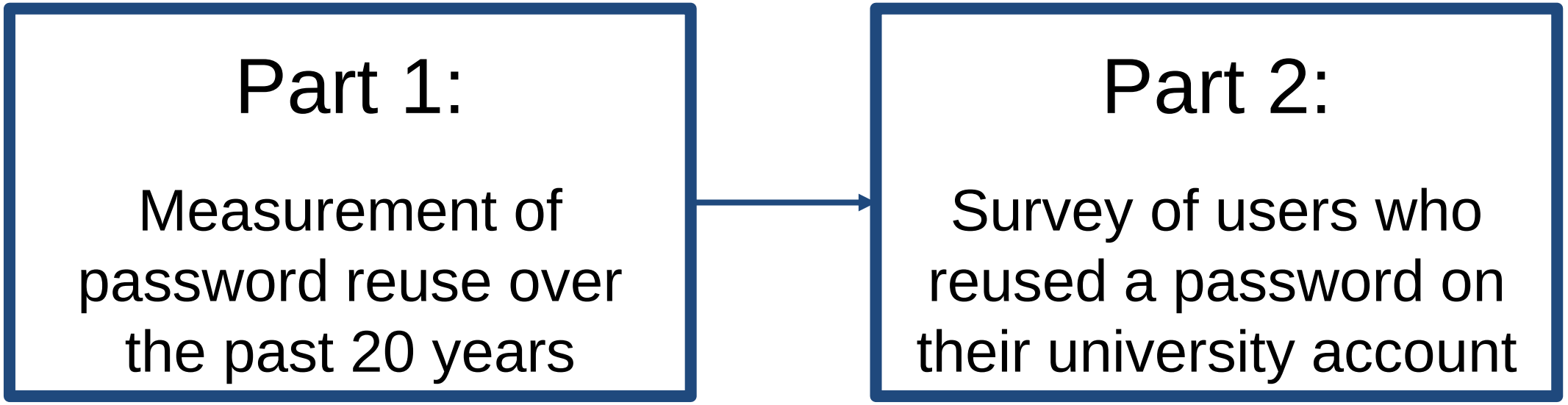
UChicago Password History Database



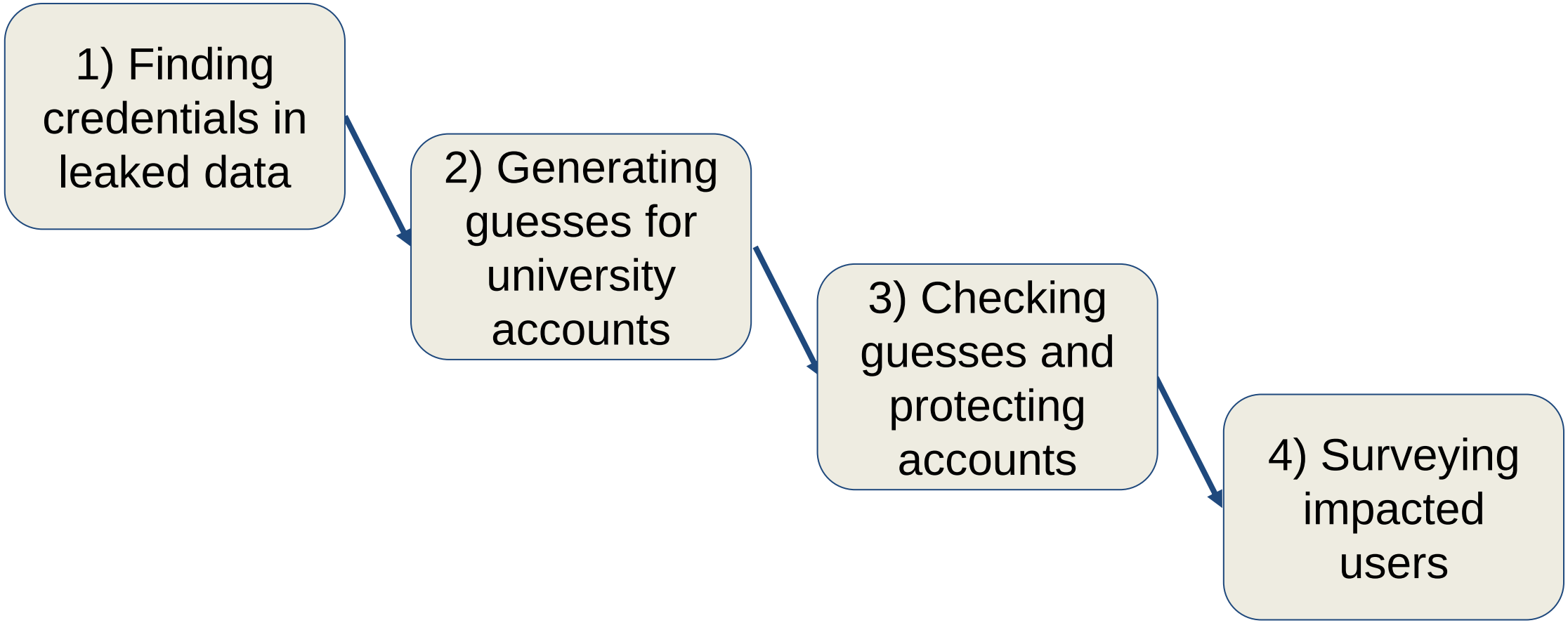
UChicago Password History Database

Username	Hash of Password	Created	Changed	
weimf	**hash(**i<3cats1234**)**	Sep 17, 2016	Jul 1, 2019	…
weimf	**hash(**i<3cats2019!**)**	Jul 1, 2019	present	…
hszym	**hash(**p@nc@kes99**)**	Aug 15, 2018	present	…
blase	**hash(**cyb#rS3curity**)**	Nov 10, 2017	Aug 23, 2019	…
…	…	…	…	…

Study Flow


Part 1:
Measurement of password reuse over the past 20 years
Part 2:
Survey of users who reused a password on their university account

Study Flow


1) Finding credentials in leaked data
2) Generating guesses for university accounts
3) Checking guesses and protecting accounts
4) Surveying impacted users

Study Flow

1) Finding credentials in leaked data

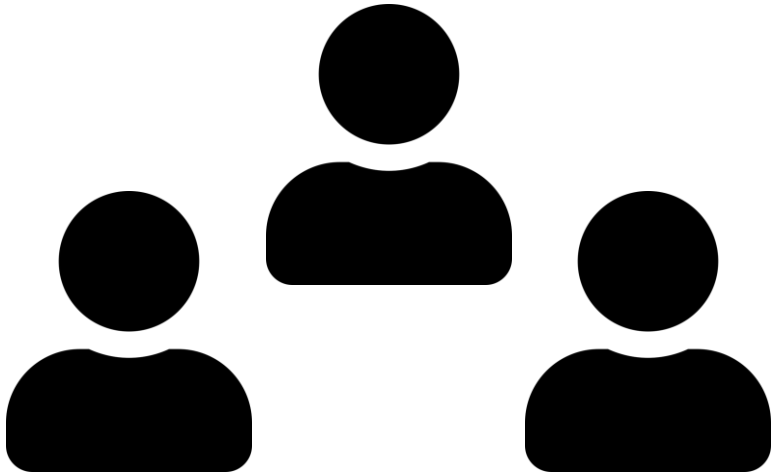
2) Generating guesses for university accounts

3) Checking guesses and protecting accounts

4) Surveying impacted users

Starting Point: UChicago Usernames

1) Finding credentials in leaked data



227,976 Usernames

Data Source 1: Data Breaches

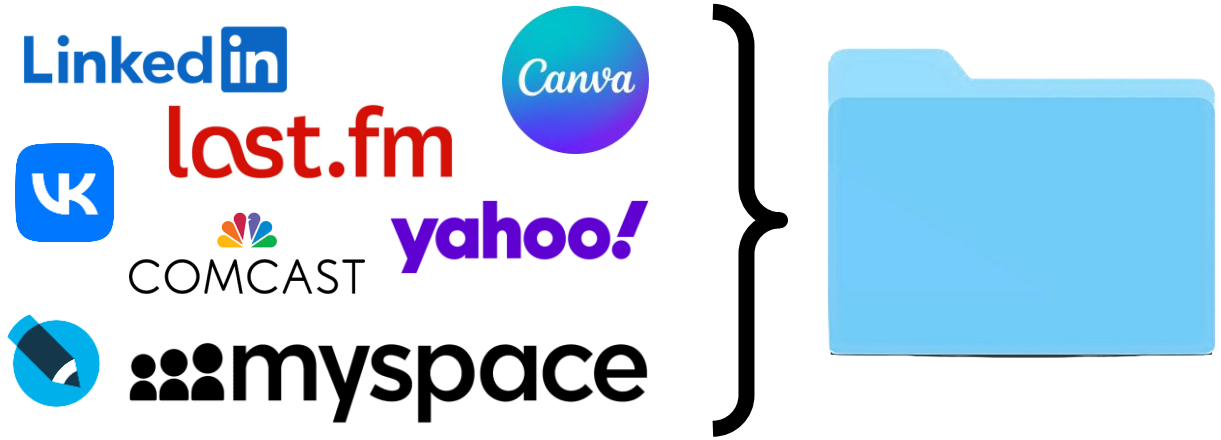
1) Finding credentials in leaked data

- 450 individual service breaches

Data Source 2: Breach Compilations

1) Finding credentials in leaked data

- 12 large breach compilations
  - Collection #1, Anti Public, etc.



Matching Strategies

1) Finding credentials in leaked data

username: **blase**

blase@uchicago.edu

blase@cmu.edu

blase

blase99@gmail.com

Study Flow

1) Finding credentials in leaked data

2) Generating guesses for university accounts

3) Checking guesses and protecting accounts

4) Surveying impacted users

Compliance With Historical Password Policies

2) Generating guesses for university accounts

	Time Period	Length	Character Classes
Password	2015 - Present	12 - 19	3+
	2010 - 2015	8 - 16	3+
	Prior to 2010	8 - 16	2+
Passphrase	2016 - Present	18 - 32	1+
	2014 - 2016	18 - 50	1+

Guessing Common Passwords

2) Generating guesses for university accounts

`password1`	→	`password1`
`LinkedIn1`	→	`UChicago1`
`P@ssw0rd1234`	→	`P@ssw0rd1234`

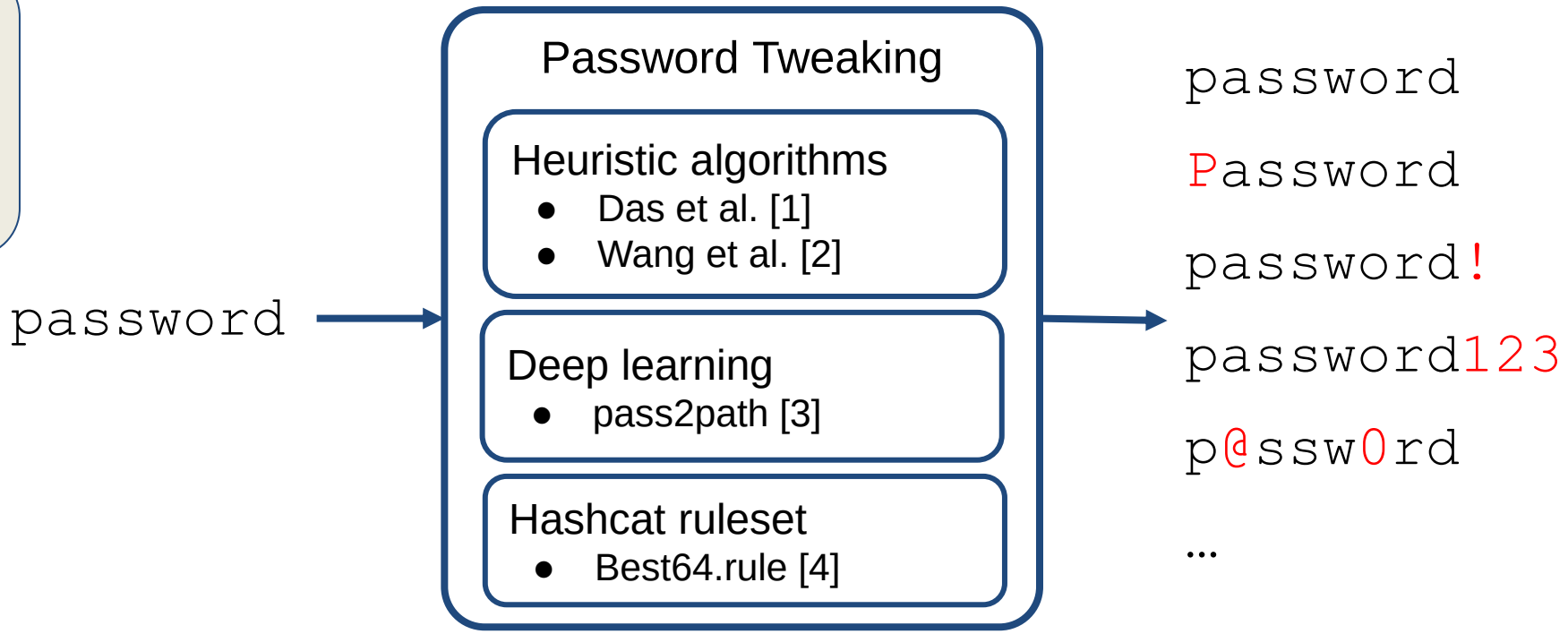
Guessing Common Passwords

2) Generating guesses for university accounts


```
password1   ──────────►  password1
LinkedIn1   ──────────►  UChicago1
P@ssw0rd1234 ─────────►  P@ssw0rd1234
```

Tweaking Guesses (Similar Passwords)

2) Generating guesses for university accounts



[1] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The Tangled Web of Password Reuse. In *Symposium on Network and Distributed System Security*, NDSS, 2014.
[2] C. Wang, S.Jan, H. Hu, D. Bossart, and G. Wang. The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services. CODASPY, 2018.
[3] B. Pal, T. Daniel, R. Chatterjee, and T. Ristenpart. Beyond Credential Stuffing: Password Similarity Models using Neural Networks. IEEE SP , 2019.
[4] J. Steube ("atom") and Community. Official Best64 Challenge Thread, 2012. https://hashcat.net/forum/thread-1002- post-5284.html#pid5284

Study Flow

1) Finding credentials in leaked data

2) Generating guesses for university accounts

3) Checking guesses and protecting accounts

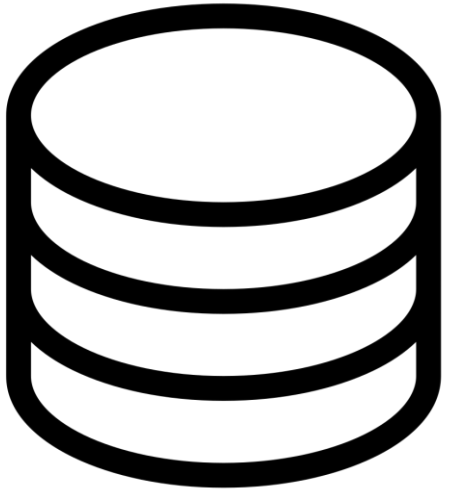
4) Surveying impacted users

Transferring Guesses

3) Checking guesses and protecting accounts

Username	Password	…
nisenoff	letmein123	…
blase	qwerty123	…
mgolla	Monkey<3	…
…	…	…

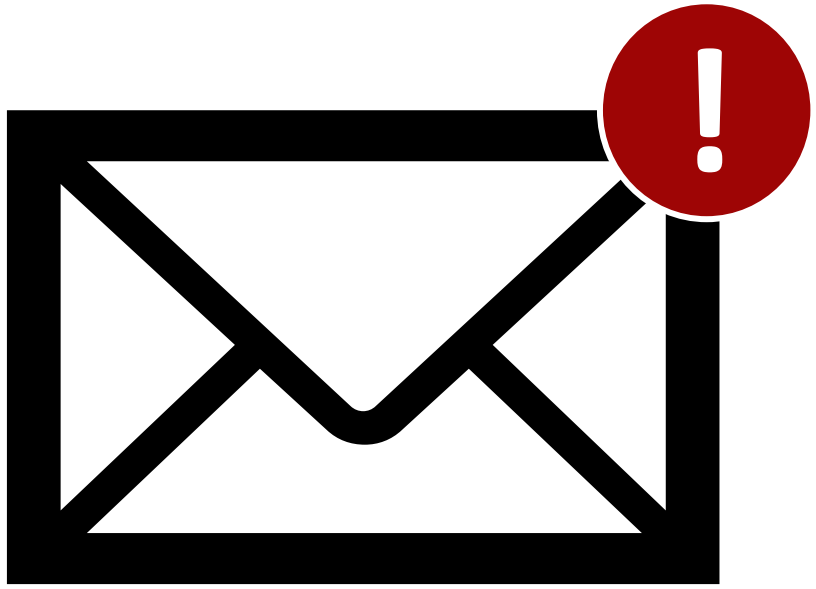
Credential Guesses



UChicago Password History Database

Notifying Vulnerable Users

3) Checking guesses and protecting accounts



Study Flow

1) Finding credentials in leaked data

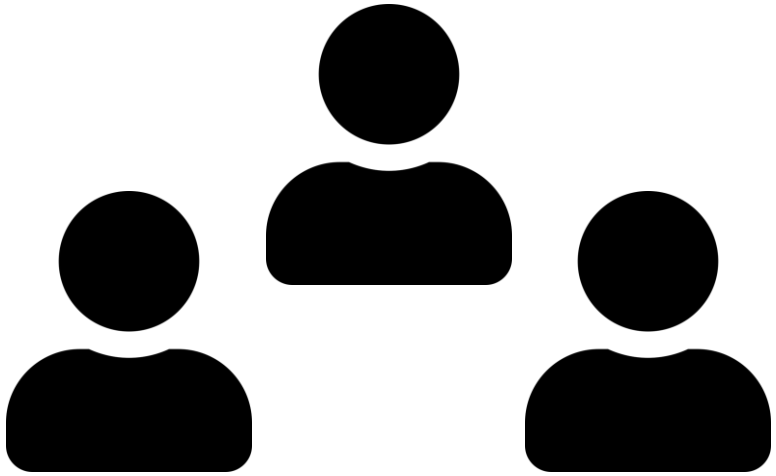
2) Generating guesses for university accounts

3) Checking guesses and protecting accounts

4) Surveying impacted users

Survey Users

4) Surveying impacted users



40 participants

Ethical Considerations

- Approved by IRB
- Study design informed by discussions with:
  - IT Leadership
  - Provost's office
  - Communications team
  - Alumni association
- Minimizing access to password history database
- Password resets to protect UChicago users

Results

12,247 correct guesses
based on password reuse

Results

We guessed at least one password for:

Results

We guessed at least one password for:

- **4.5%** of all users in the password history database

Results

We guessed at least one password for:

- **4.5%** of all users in the password history database
- **6.5%** of users for whom we made a guess

Results

We guessed at least one password for:

- **4.5%** of all users in the password history database
- **6.5%** of users for whom we made a guess
- **32.0%** of users with a uchicago.edu email in a data breach

Results

We guessed the current password for

3,618 accounts

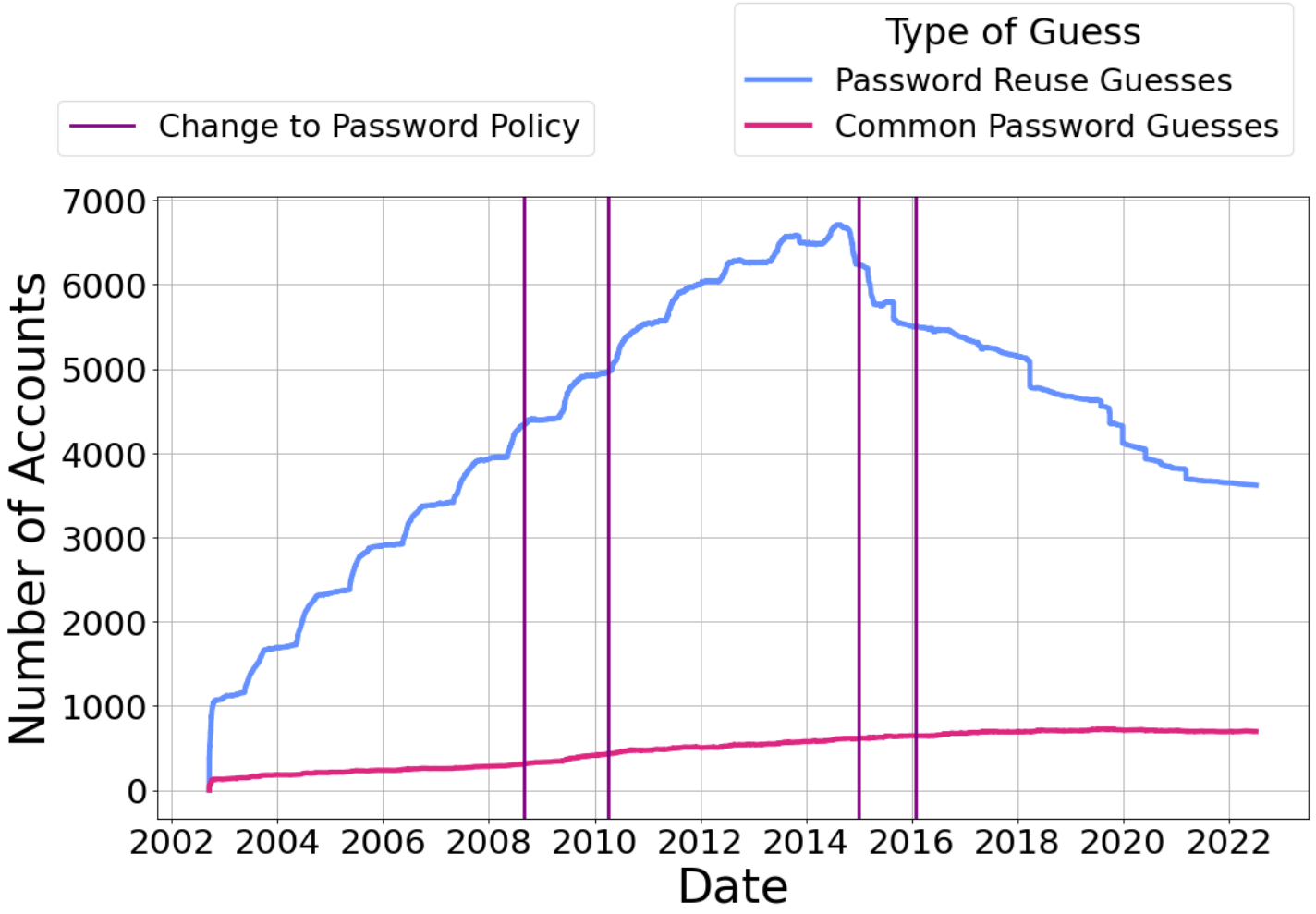
Sources of Correct Guesses

71 individual service breaches

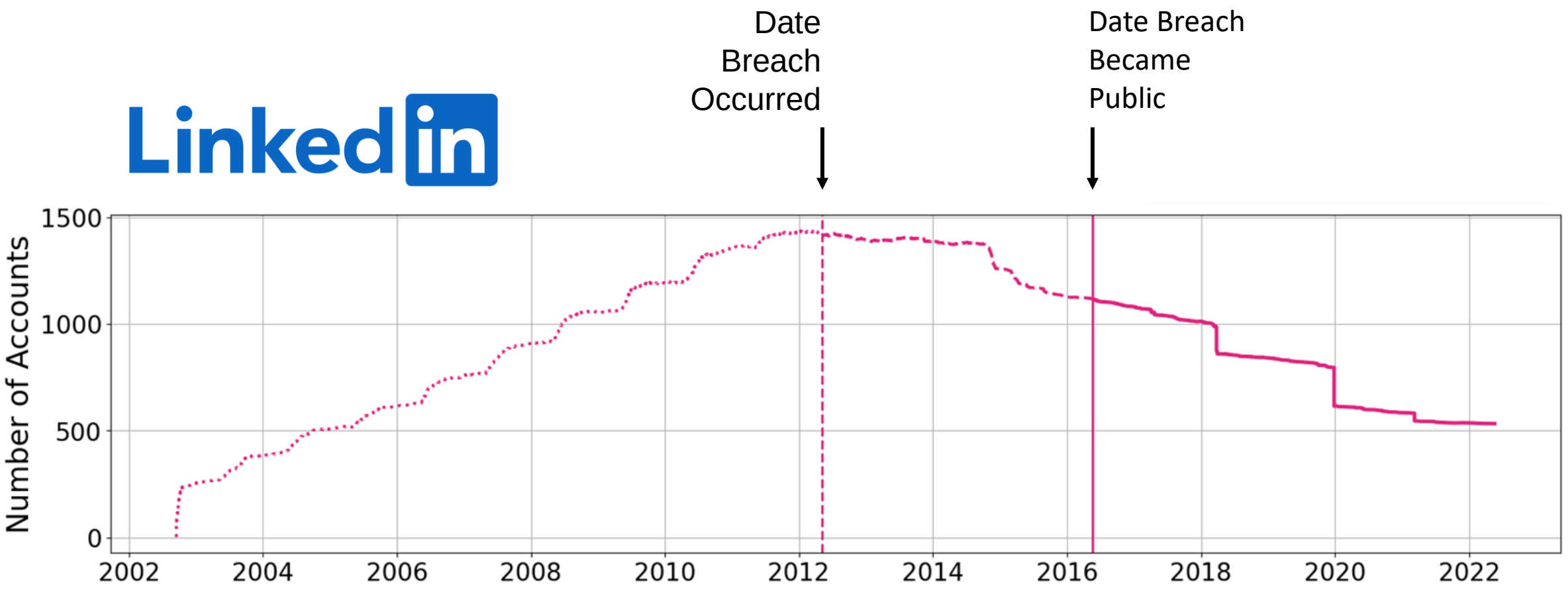
Sources of Correct Guesses

71 individual service breaches
…and all 12 breach compilations

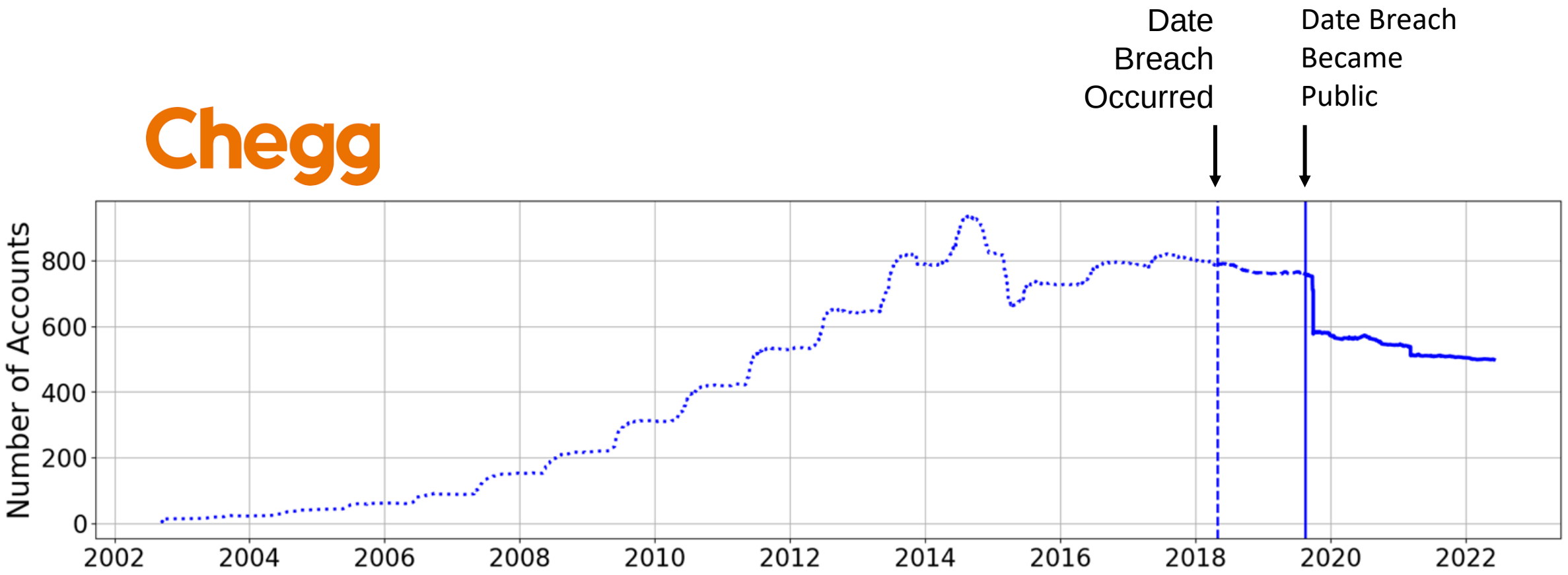
Number of Vulnerable Accounts Over Time



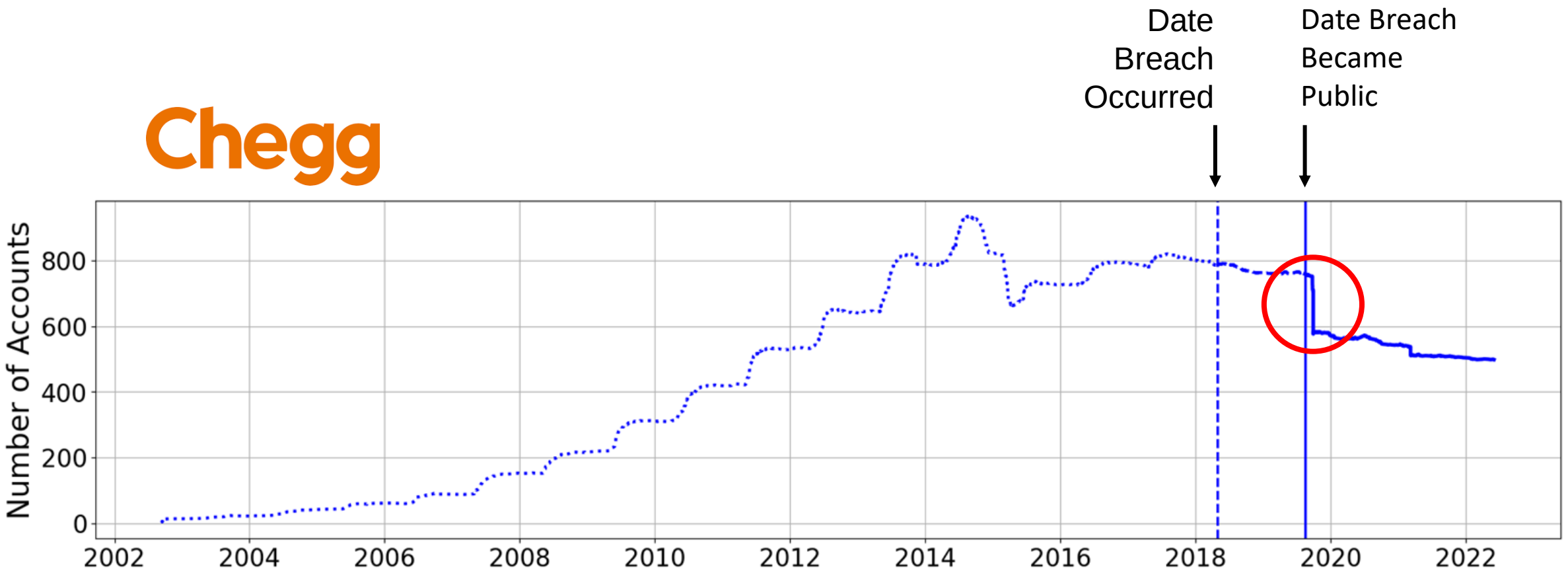
Some Accounts Remained Vulnerable For Years



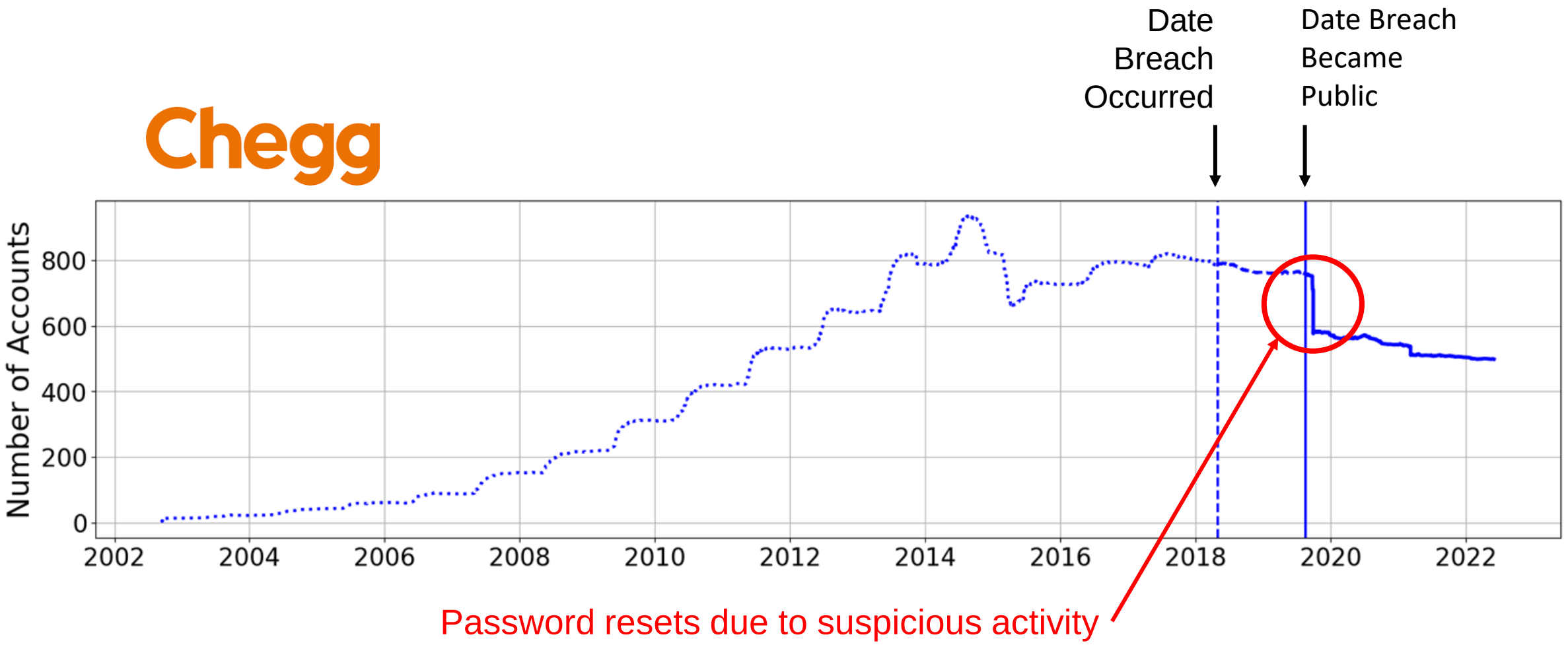
Some Accounts Were Quickly Exploited



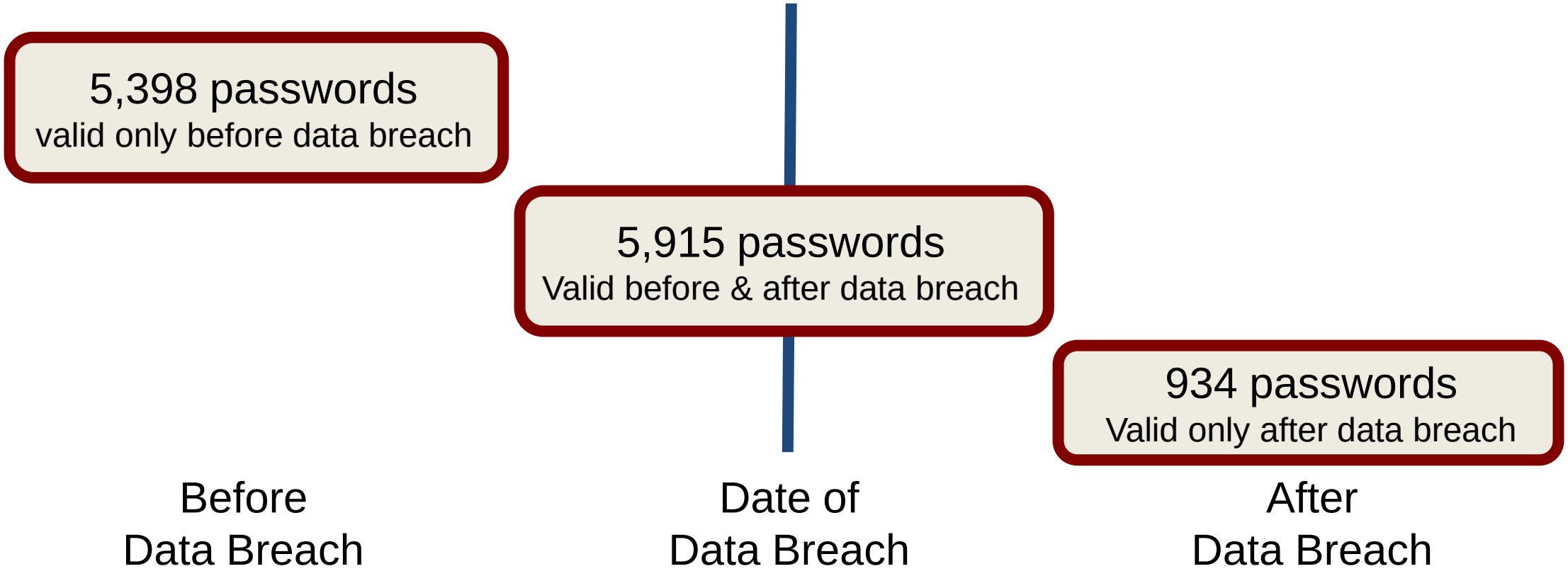
Some Accounts Were Quickly Exploited



Some Accounts Were Quickly Exploited



Passwords Created at UChicago Before Breach



Impact on Specific User Groups

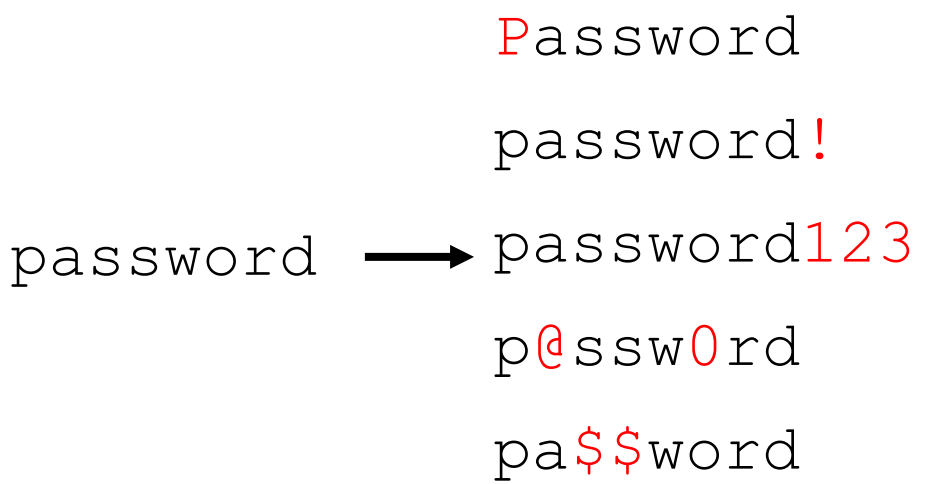
	LinkedIn	Chegg
Students	11.2%	41.4%
Faculty	54.3%	2.2%

Importance of Cracking Hashes

Plaintext	Hashed
85.3%	14.7%
Sunshine!	5F4DCC3B5AA765D61D8327DEB882CF99
correctbatteryhorsestaple	482C811DA5D5B4BC6D497FFA98491E38
i@mforg3tful!	62099D23A9D9910879D67449D9E084ED
ineedapassword	1C8F93D67A694EE1DE6363D20228DAC8

Importance of Tweaking Guesses

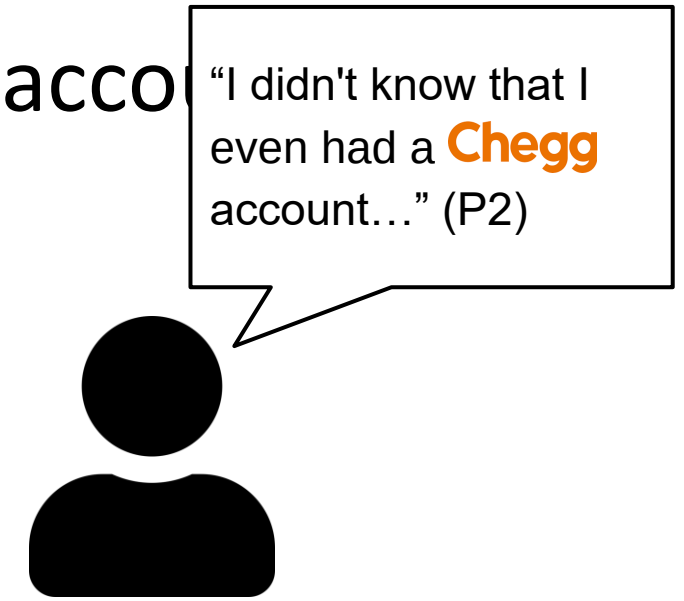
Verbatim Reuse 54.7%



Tweaked Passwords 45.3%

User Reactions and Experiences (N = 40)

- Users are aware they are reusing passwords
- Users know about some, but not all, relevant breaches
- Some users were unaware they had acco
  that had suffered a data breach



Key Recommendations for Organizations

Implement processes to expire unused accounts

';- HIBP

Using credential checking services when passwords are created is not enough

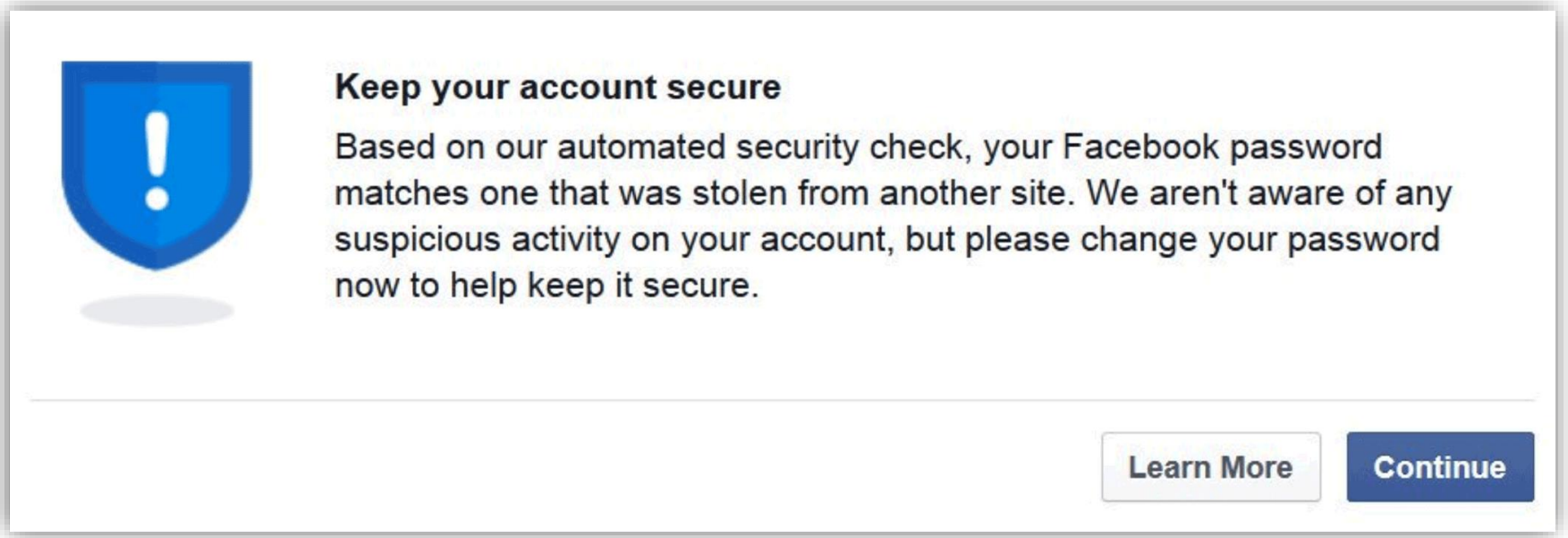
Promptly check high-risk breaches when they become public

Check for reuse of hashed and tweaked passwords in less common data breaches

fido™

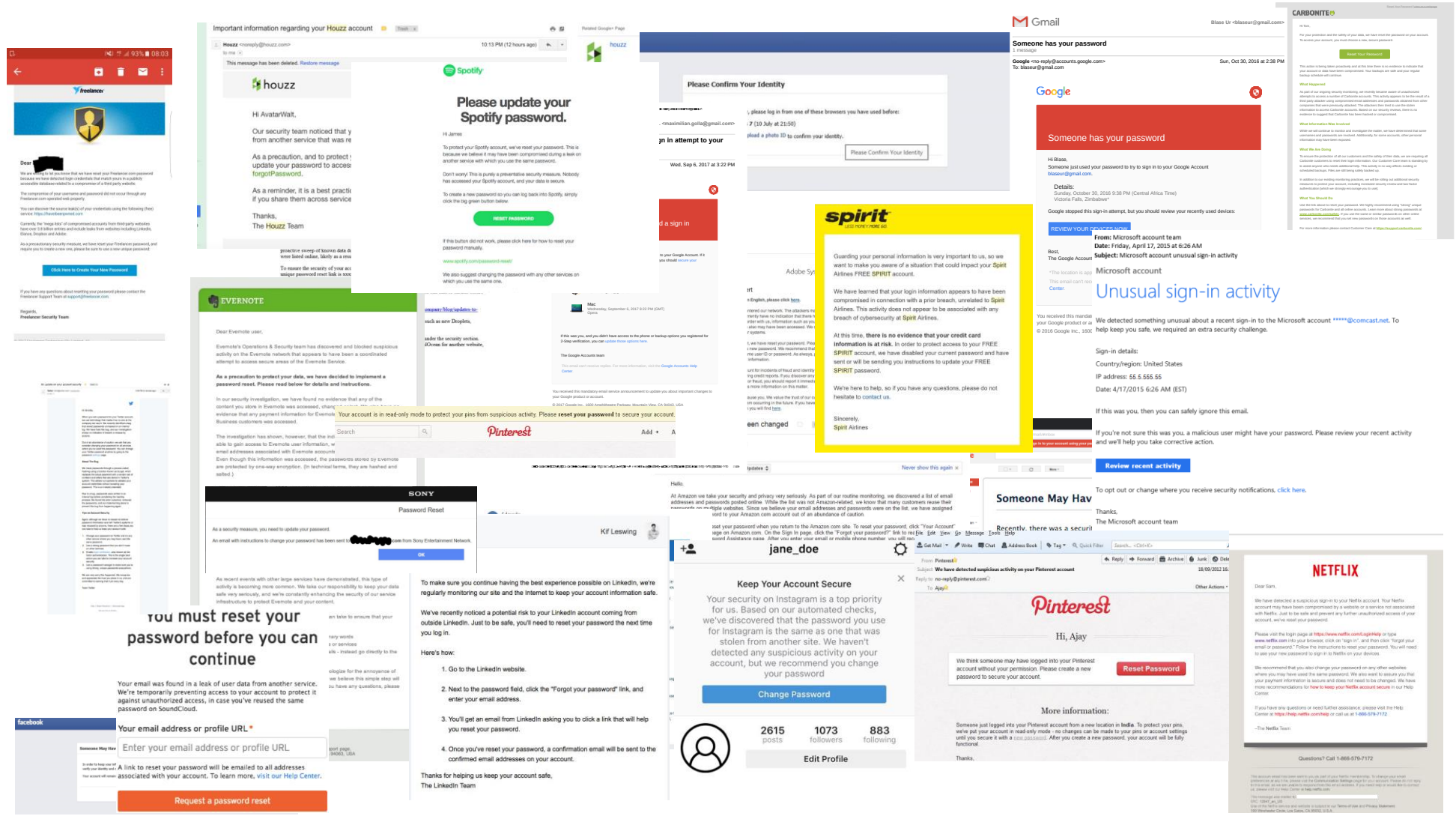
Use 2FA and consider moving to FIDO2 Passwordless Authentication

Notifying Users About Password Reuse



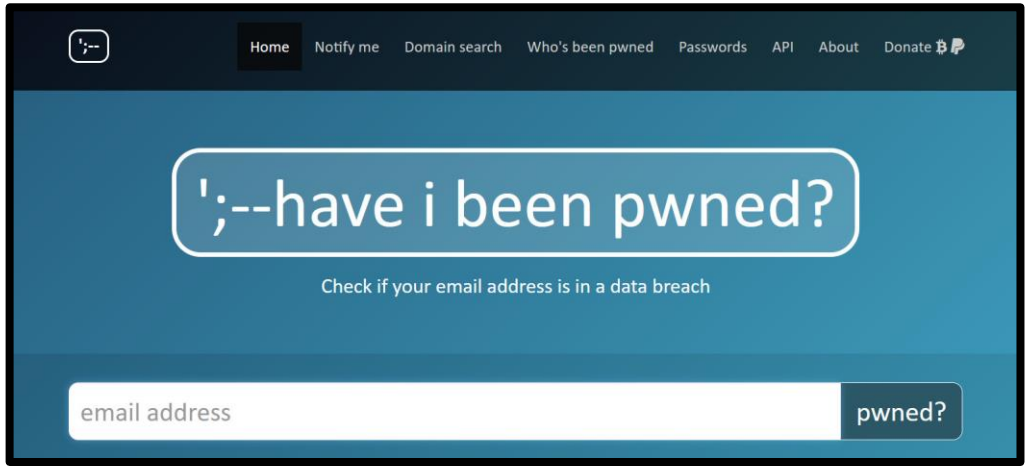
Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, Blase Ur. “What was that site doing with my Facebook Password?” Designing Password-Reuse Notifications. In *Proc. CCS*, 2018.

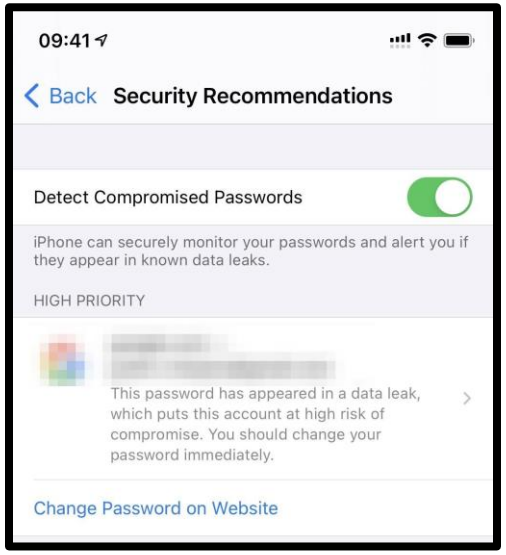
Password-Reuse Notifications

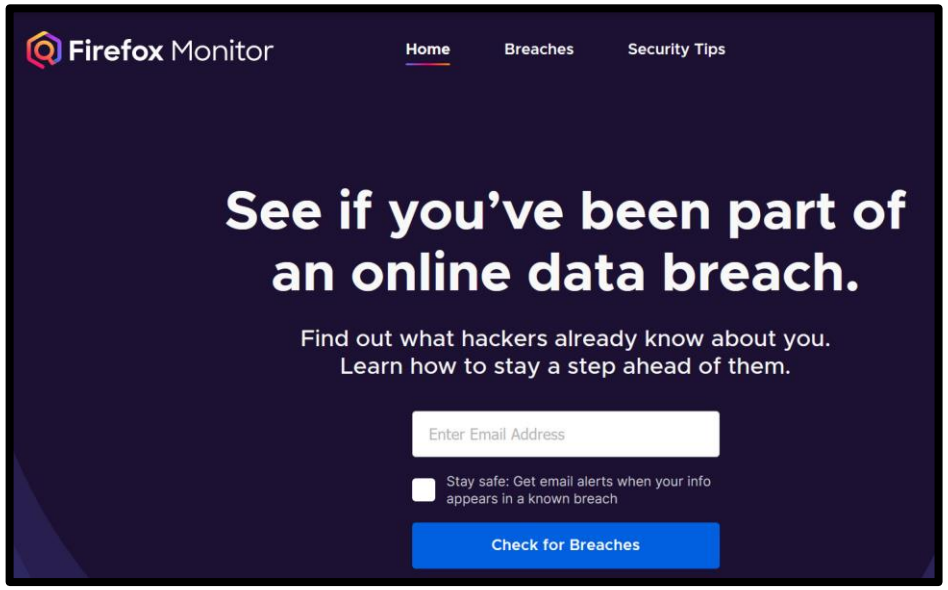


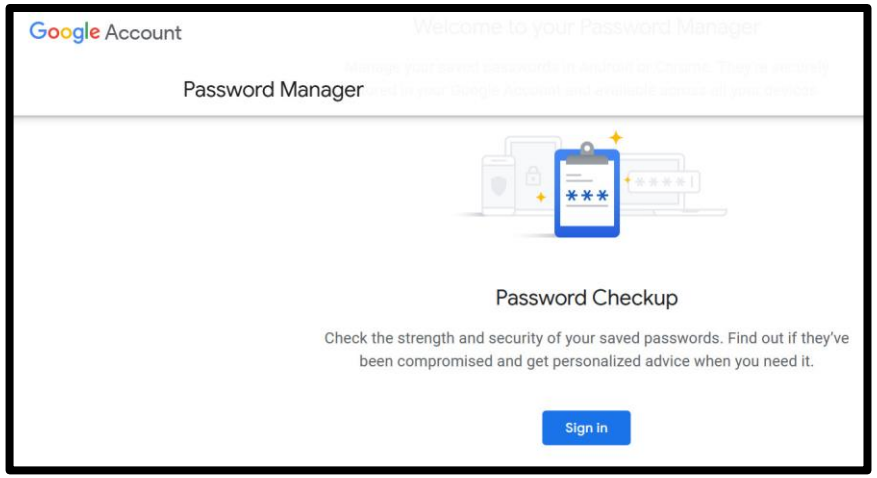
Authentication in Practice: Checking for Compromised Credentials

Checking for Compromised Credentials









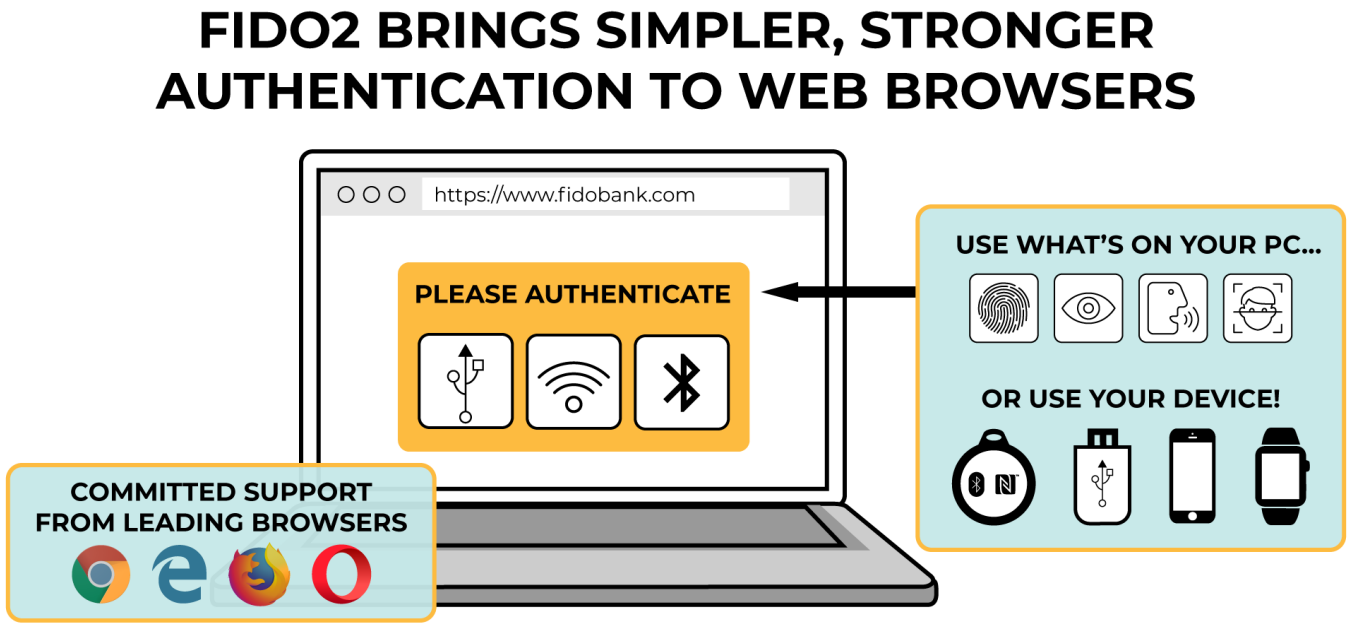
https://www.zdnet.com/article/google-launches-password-checkup-feature-will-add-it-to-chrome-later-this-year/
https://ios.gadgethacks.com/how-to/ios-14-monitors-your-passwords-protect-you-against-data-breaches-heres-works-0341281/

Checking for Compromised Credentials

https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html

Authentication in Practice: Moving Towards A Passwordless World?

Passwordless FIDO2



Passwordless FIDO2

- Goal: Authenticate on web using public-key crypto
- Created by the FIDO Alliance, now a W3C standard
  - https://www.w3.org/TR/webauthn-2/
- Originally intended to be implemented in specialized hardware OR in software using a TPM/TEE

Passwordless FIDO2: WebAuthn Protocol

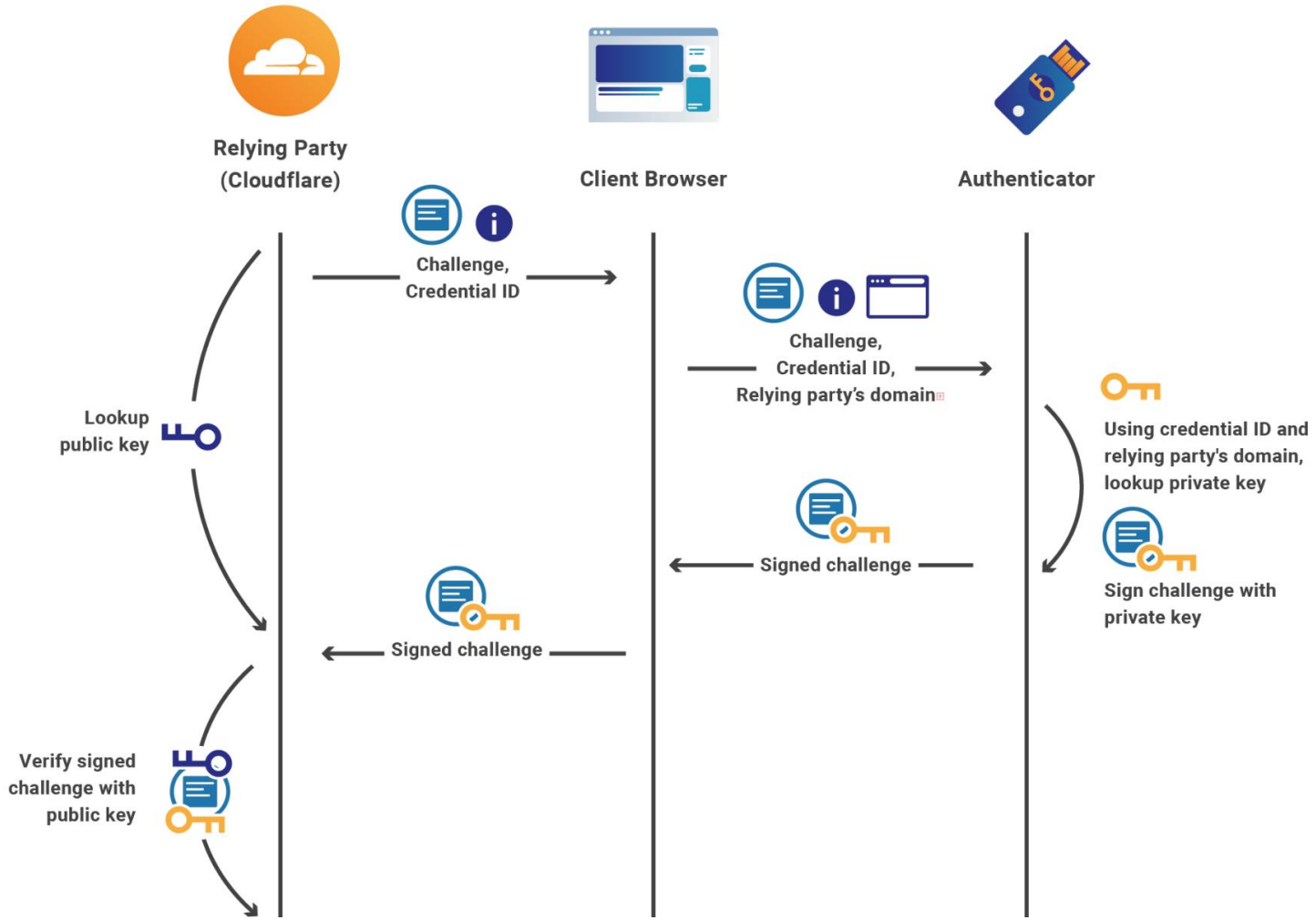


Image from https://blog.cloudflare.com/cloudflare-now-supports-security-keys-with-web-authentication-webauthn

Integrating WebAuthn With Okta

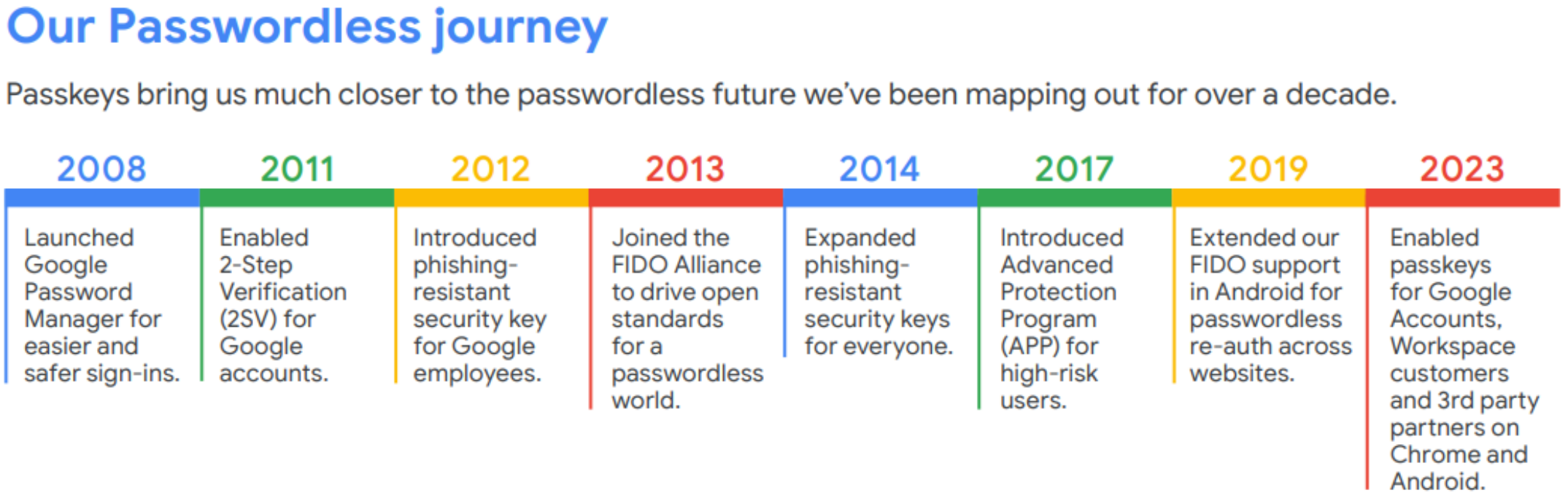
Image from https://developer.okta.com/docs/guides/authenticators-web-authn/main/

Passwordless FIDO2: User Interaction

- Type a PIN into the device, present biometric (fingerprint) to hardware reader, or press a button on the key

Passkeys

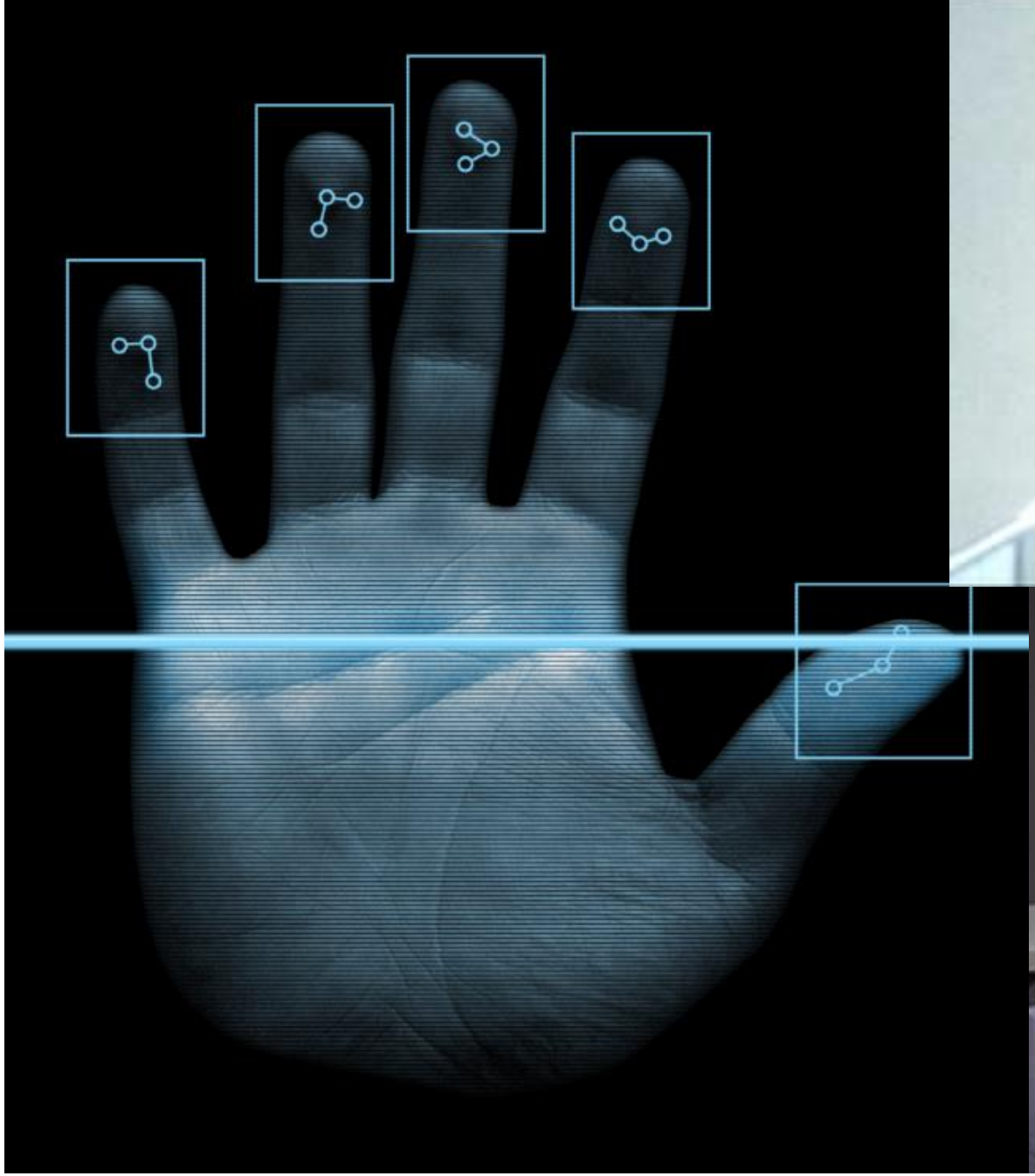
- Goal: Make FIDO2 / WebAuthn more usable by syncing the private key across devices
  - See: https://developers.google.com/identity/passkeys
  - Example of Google's changing approach over the years:



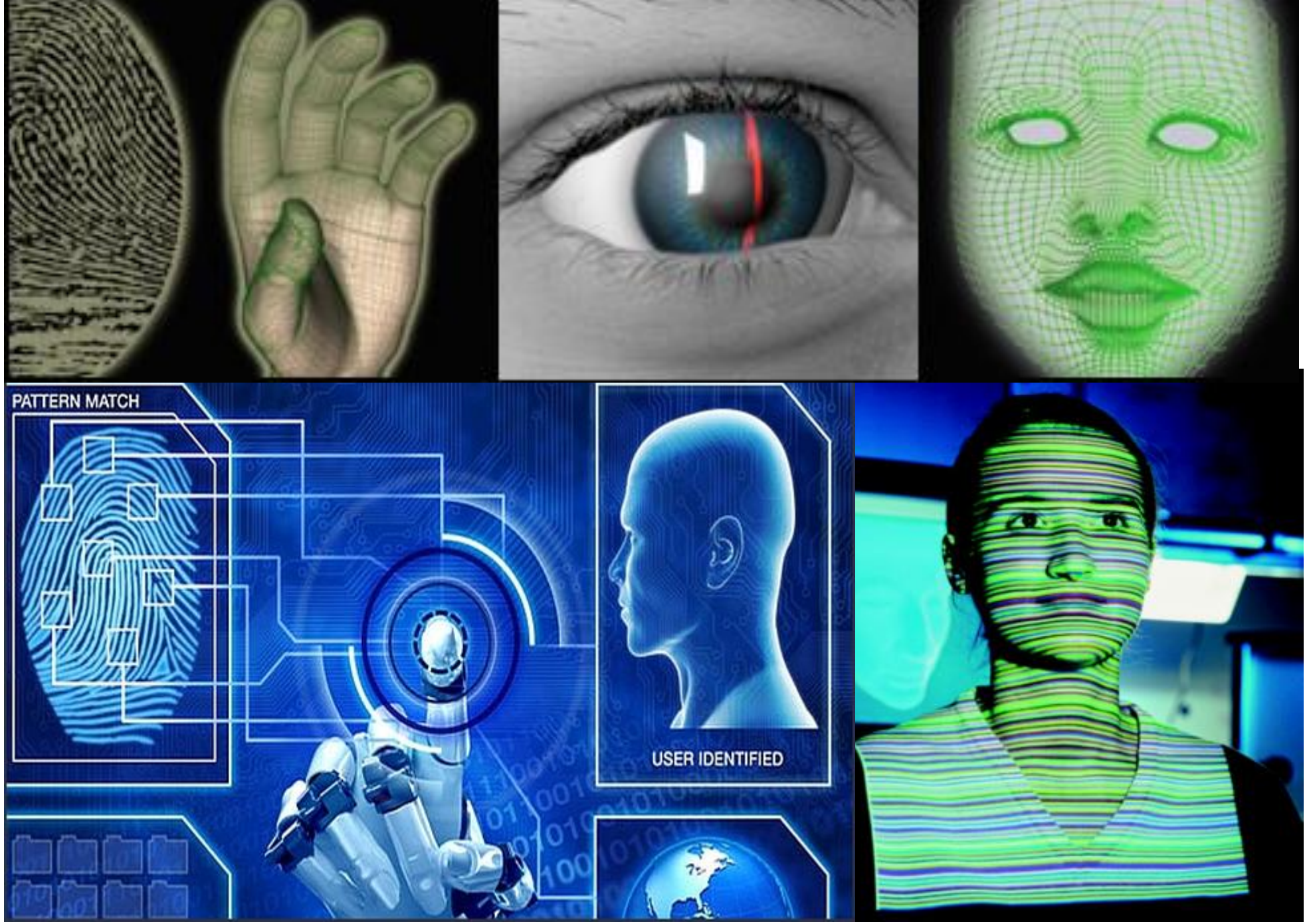
What about Biometrics?

•Images on previous slide fair use from androidcentral.com and businessinsider.com. Photo above fair use from abcnews.com

•Images fair use from wordpress.com and kaspersky.com, as well as Creative Commons from matsuyuki on Flickr



•Images fair use from ccmcinc.com, filmjunk.com, and discovermagazine.com



Images fair use from fbi.gov, ifsecglobal.com, and siemens.com

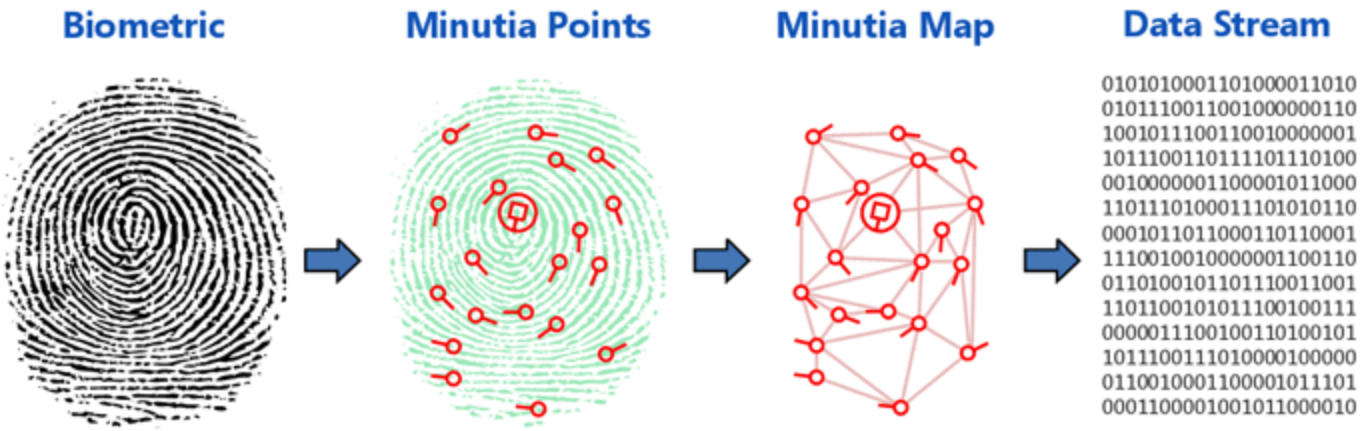
Biometrics

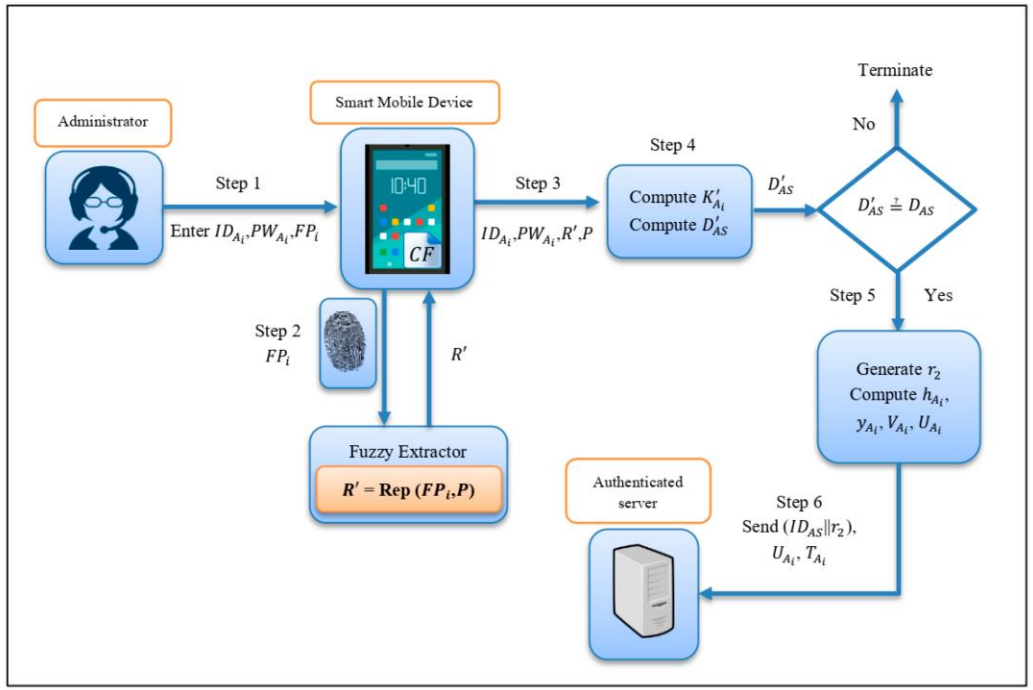
- Fingerprint
- Iris scans or retina scans
- Face recognition
- Finger/hand geometry
- Voice or speech recognition
- The way you type
- (Many others)

Practical Challenges for Biometrics

- Immutable (can’t be changed)
- Potentially sensitive data
- High equipment costs
- Sensitive to changes in the environment
- Biometrics can change over time

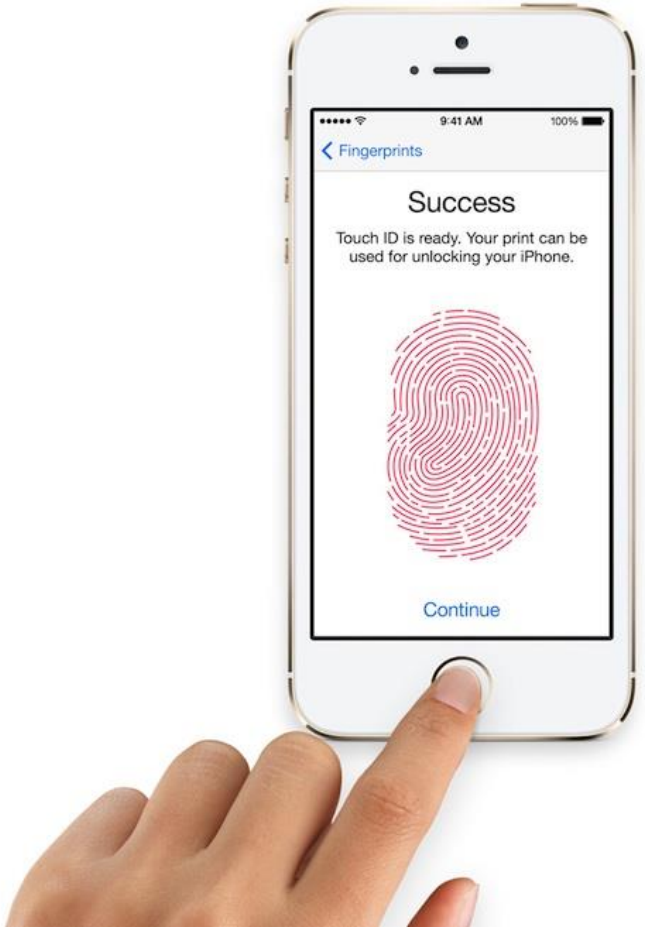
Storing Biometrics: Templates





Smartphone Biometrics

- Purpose is to reduce the number of times a user must enter their password
- Falls back to the password
- Some facial recognition systems can be tricked by a photo
- Some fingerprint recognition systems can be tricked by a gummy mold



•Images fair use from creativebits.org, and businessinsider.com.