

# 14. Authentication

## Part 2



Blase Ur and Grant Ho  
February 21<sup>st</sup>, 2024  
CMSC 23200

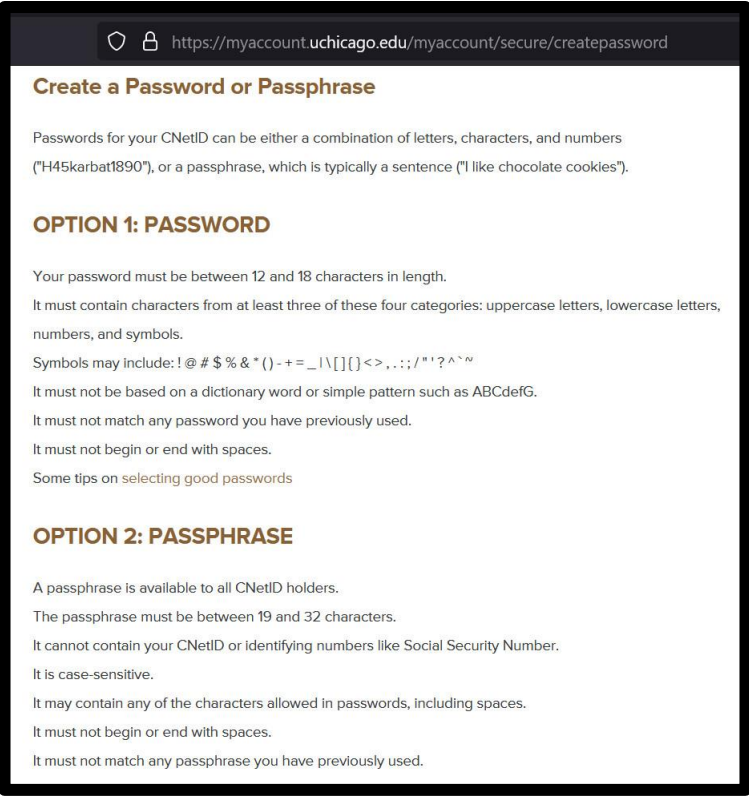


THE UNIVERSITY OF  
CHICAGO

How Do We Help Users  
Make Better Passwords?

# Password-Composition Rules

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



The screenshot shows a web browser window with the address bar displaying `https://myaccount.uchicago.edu/myaccount/secure/createpassword`. The page title is "Create a Password or Passphrase". Below the title, there is a paragraph explaining that passwords can be a combination of letters, characters, and numbers, or a passphrase (a sentence). The page is divided into two sections: "OPTION 1: PASSWORD" and "OPTION 2: PASSPHRASE".

**Create a Password or Passphrase**

Passwords for your CNetID can be either a combination of letters, characters, and numbers ("H45karbat1890"), or a passphrase, which is typically a sentence ("I like chocolate cookies").

**OPTION 1: PASSWORD**

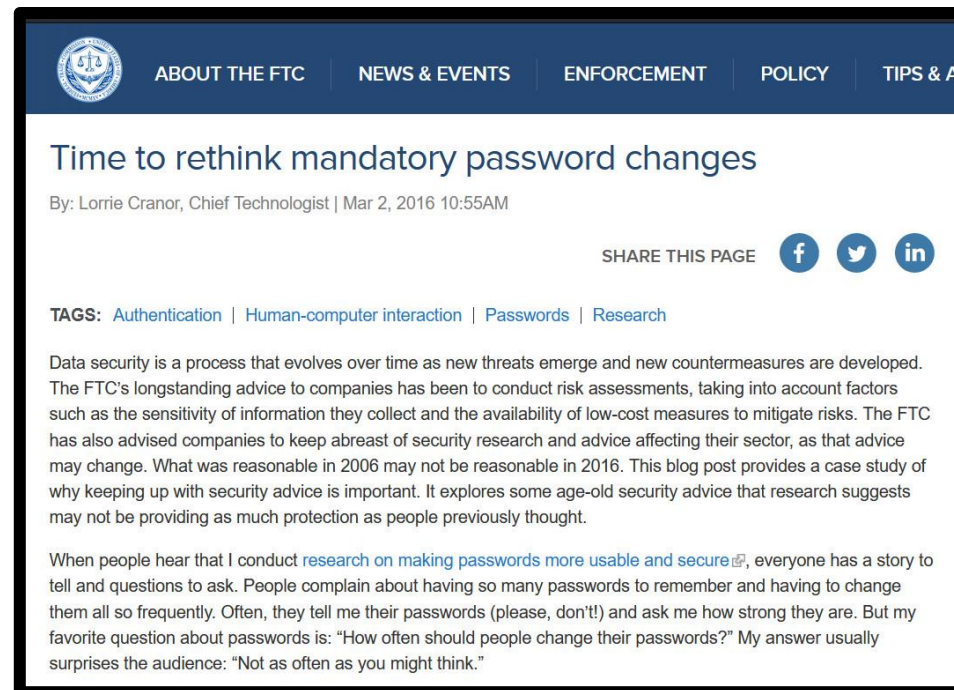
Your password must be between 12 and 18 characters in length.  
It must contain characters from at least three of these four categories: uppercase letters, lowercase letters, numbers, and symbols.  
Symbols may include: ! @ # \$ % & \* ( ) - + = \_ ! \ [ ] { } < > , . : ; / ' ' ? ^ ~ `"  
It must not be based on a dictionary word or simple pattern such as ABCdefG.  
It must not match any password you have previously used.  
It must not begin or end with spaces.  
[Some tips on selecting good passwords](#)

**OPTION 2: PASSPHRASE**

A passphrase is available to all CNetID holders.  
The passphrase must be between 19 and 32 characters.  
It cannot contain your CNetID or identifying numbers like Social Security Number.  
It is case-sensitive.  
It may contain any of the characters allowed in passwords, including spaces.  
It must not begin or end with spaces.  
It must not match any passphrase you have previously used.

# 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.

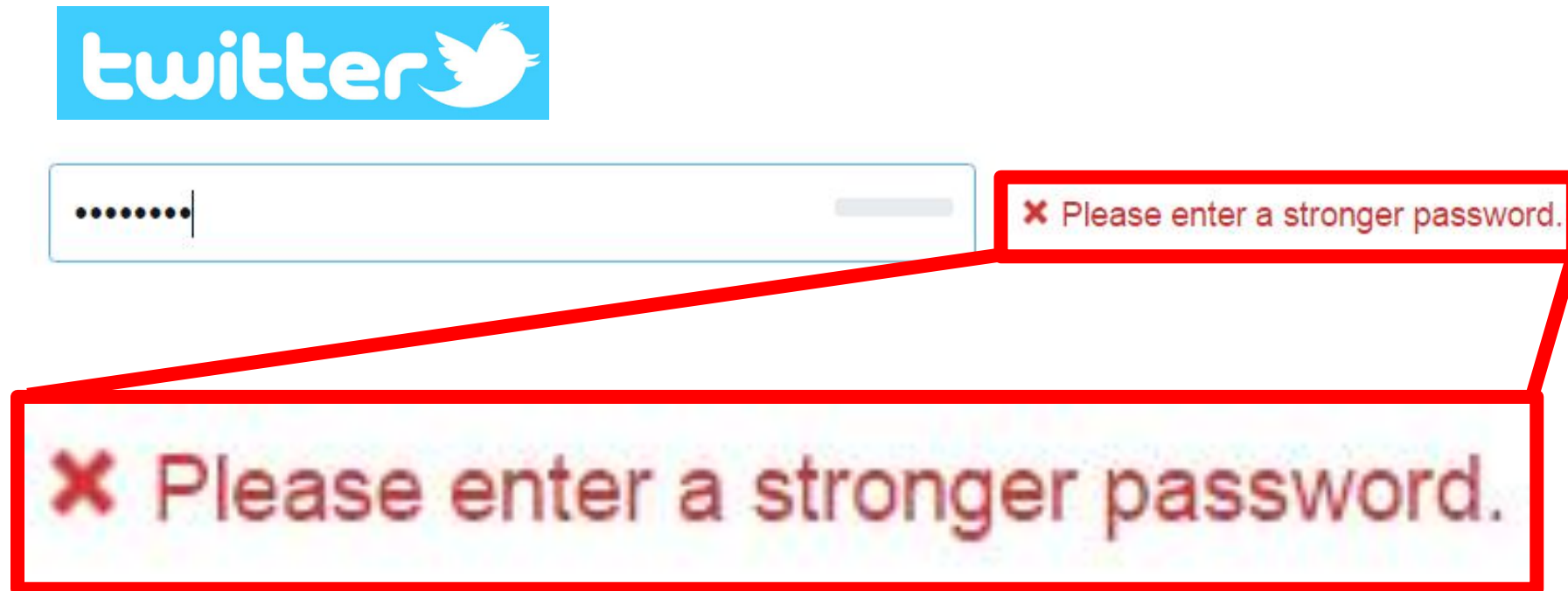
## Problem 2: Inaccurate Feedback



Password1!



# Problem 3: Unhelpful Feedback



The image shows a Twitter login form. At the top is the Twitter logo. Below it is a text input field for a password, represented by dots. To the right of the input field is a small error message: "✗ Please enter a stronger password." A red line connects this message to a larger, magnified version of the same message below it, illustrating that the feedback is unhelpful because it does not provide any specific guidance on how to create a stronger password.

twitter

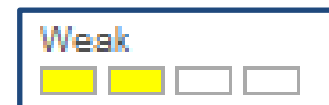
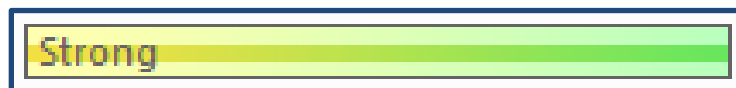
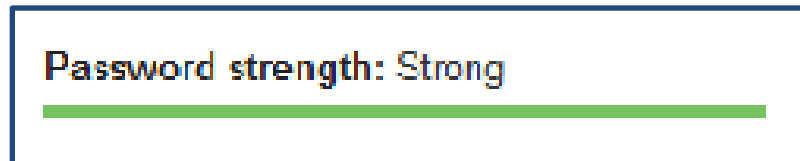
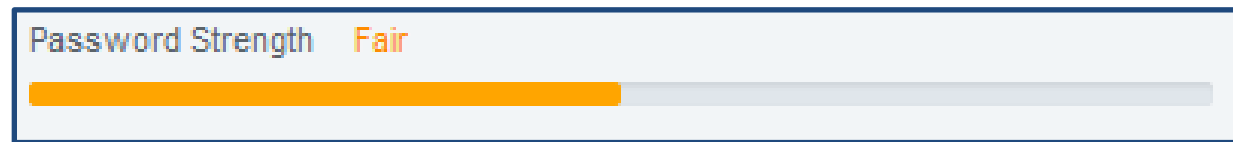
.....

✗ Please enter a stronger password.

✗ Please enter a stronger password.

# Proactive Strength Checking

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



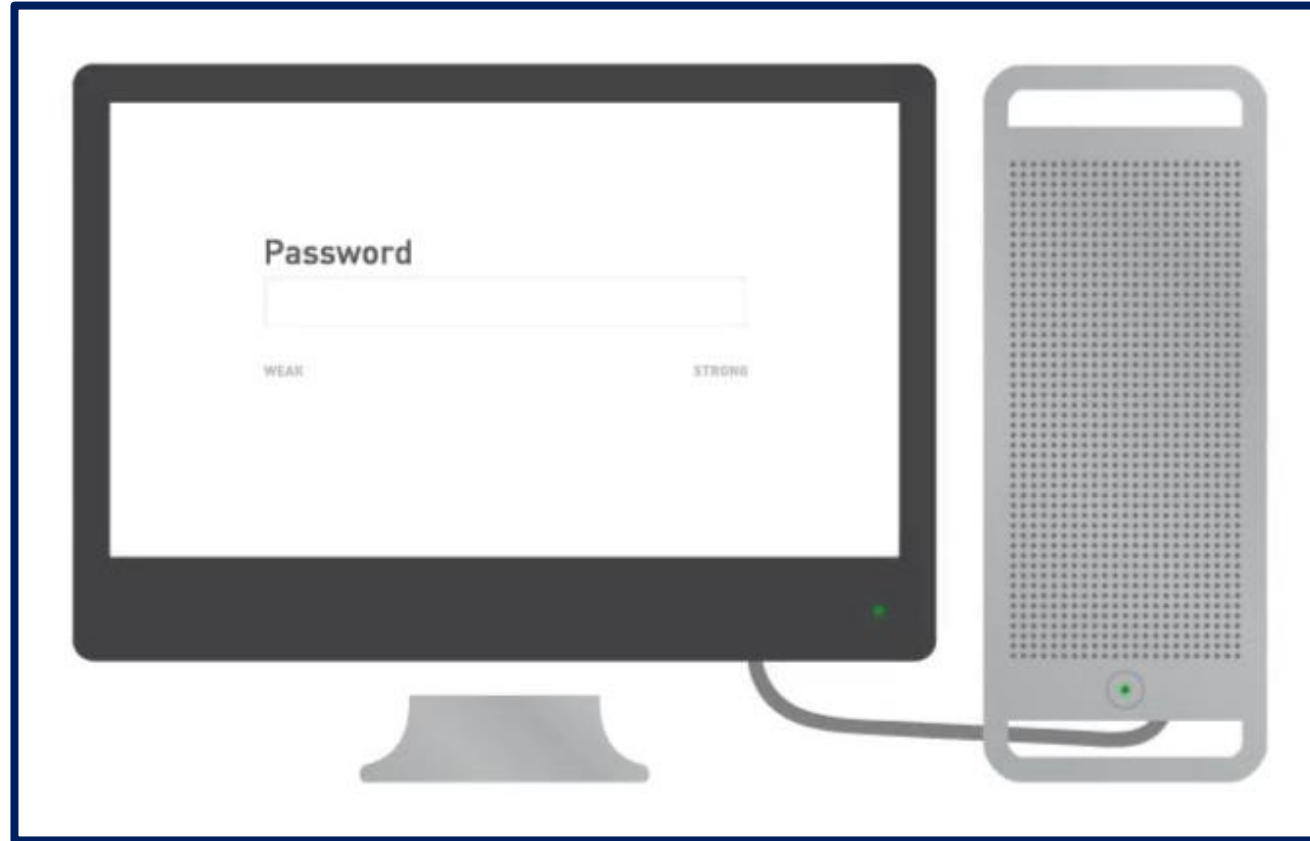


# User-Centered Security

# Some Ways to Understand Users

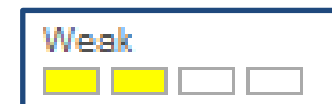
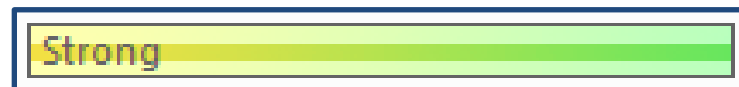
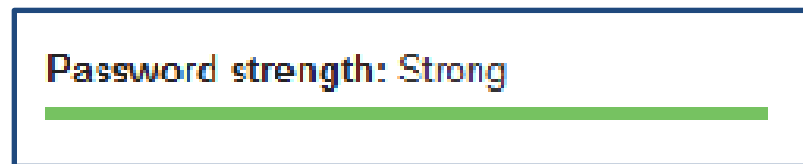
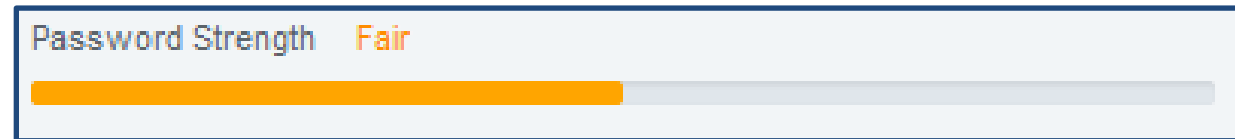
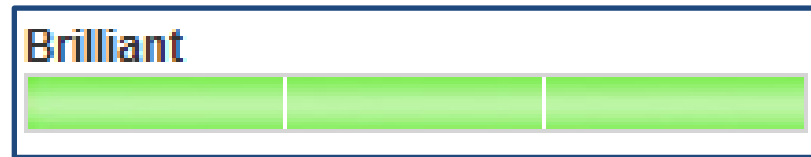
- Retrospective analysis of password breaches
- Large-scale online studies
- Examine real passwords with permission
- Qualitative studies

# 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

 LiveMail

## Create a password

Account Password

A strong password helps prevent unauthorized access to your email account.

Type new password:

8-character minimum; case sensitive

Password strength: Bad. Consider adding an uppercase letter or making your password longer.

Retype new password:

☐ Make my password expire every 72 days.

# Visual Differences

Type new password:

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:

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

Type new password:

8-character minimum; case sensitive

**Baseline meter**

Excellent!



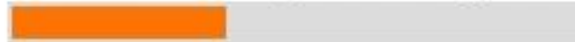
**Half-score**

Poor. Consider adding a different symbol or making your password longer.



**One-third-score**

Bad. Consider adding a different symbol or making your password longer.



**Nudge-16**

Poor. Consider making your password longer.



**Nudge-Comp8**

Excellent!



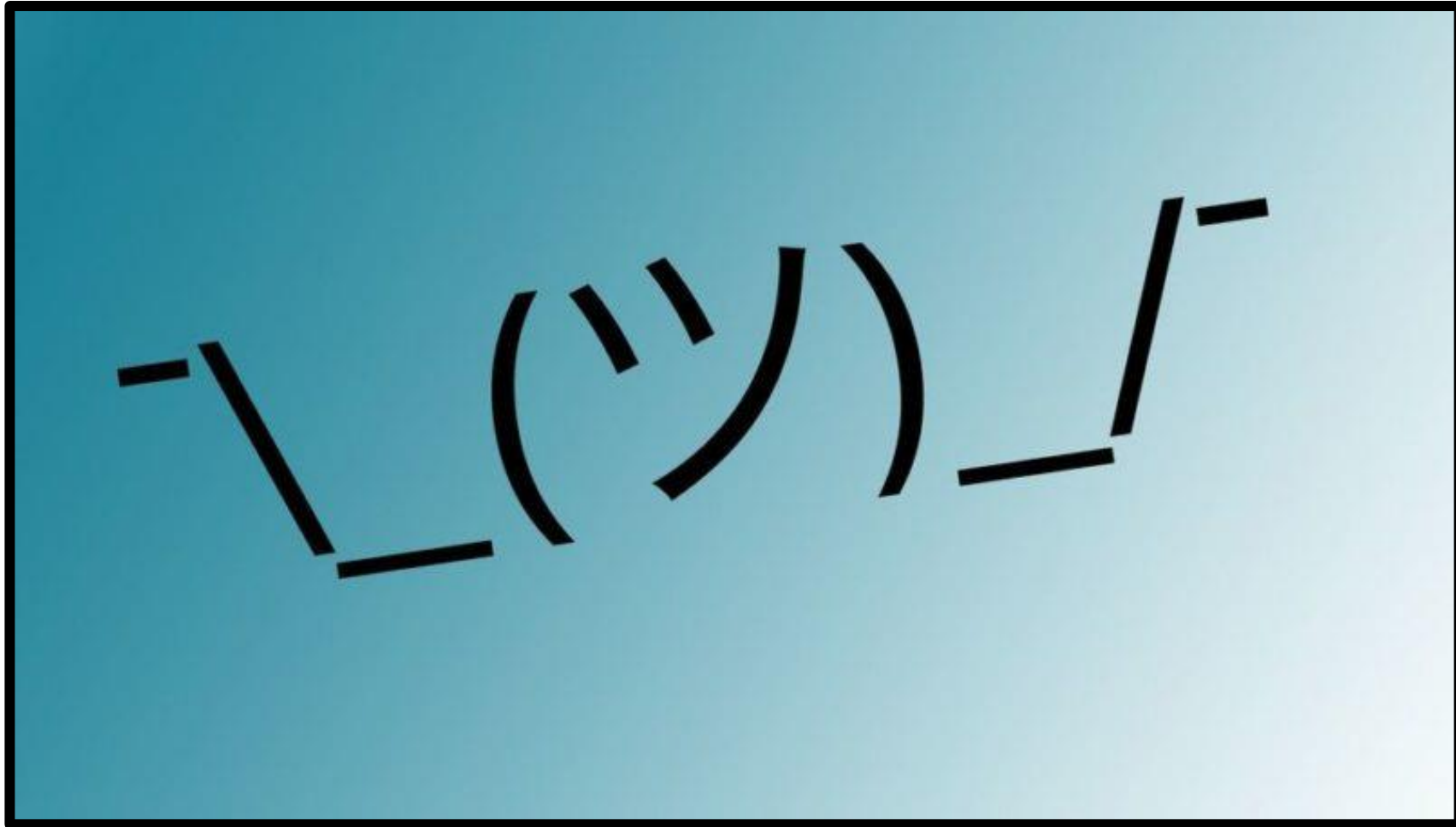
# Key Results

- 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

The screenshot shows a web form titled "Create Your Password". It contains three input fields: "Username", "Password", and "Confirm Password". The "Password" field contains the text "Mypassword123" and has a red progress bar below it. A checkbox labeled "Show Password & Detailed Feedback" is checked. A blue "Continue" button is at the bottom right. To the right of the form is a feedback panel with a grey background. It starts with the text "Your password is very easy to guess." followed by three bullet points, each with a blue square icon and a "(Why?)" link. The first bullet point says "Don't use dictionary words (password)". The second says "Capitalize a letter in the middle, rather than the first character". The third says "Consider inserting digits into the middle, not just at the end". Below these is a suggestion: "A better choice: My123passwoRzd" and a link "How to make strong passwords".

Create Your Password

Username

Password  
Mypassword123  
☐ Show Password & Detailed Feedback

Confirm Password

[Continue](#)

Your password is very easy to guess.

- Don't use dictionary words ([Why?](#))
- Capitalize a letter in the middle, rather than the first character ([Why?](#))
- Consider inserting digits into the middle, not just at the end ([Why?](#))

A better choice: My123passwoRzd

[How to make strong passwords](#)

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







- 1) Principled strength estimates (RNN)
- 2) Data-driven feedback to users







# Provide Intelligent Explanations

Unic0rns

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...

## Create Your Password

Username

blase

Password

.....

Show Password & Detailed Feedback

Confirm Password

Continue

Your password could be better.

- Don't use dictionary words or words used on Wikipedia [\(Why?\)](#)
- Consider inserting digits into the middle [\(Why?\)](#)
- Consider making your password longer [\(Why?\)](#)

See Your Password With Our Improvements

[How to make strong passwords](#)

## ...Displays Score Visually

### Create Your Password

Username

blase

Password

.....

Show Password & Detailed Feedback ☐

Confirm Password

Continue

Your password could be better.

■ Don't use dictionary words or words used on Wikipedia

(Why?)

■ Consider inserting digits into the middle

(Why?)

■ Consider making your password longer

(Why?)

See Your Password With Our Improvements

[How to make strong passwords](#)

## ...Provides Text Feedback

### Create Your Password

Username

blase

Password

.....

Show Password & Detailed Feedback

Confirm Password

Continue

Your password could be better.

■ Don't use dictionary words or words used on Wikipedia

[\(Why?\)](#)

■ Consider inserting digits into the middle

[\(Why?\)](#)

■ Consider making your password longer

[\(Why?\)](#)

See Your Password With Our Improvements

[How to make strong passwords](#)

# ...Gives Detail (Password Shown)

### Create Your Password

Username

blase

Password

CryptoUnicorn3|

Show Password & Detailed Feedback

☒

Confirm Password

Continue

Your password could be better.

- Don't use dictionary words (Unicorn) or words used on Wikipedia (Crypto) [\(Why?\)](#)
- Consider inserting digits into the middle, not just at the end [\(Why?\)](#)
- Consider making your password longer than 14 characters [\(Why?\)](#)

A better choice: C3ryptoUniCorn@

[How to make strong passwords](#)

# ...Offers Explanations

### Create Your Password

Username

blase

Password

CryptoUnicorn3|

Show Password & Detailed Feedback

☒

Confirm Password

Continue

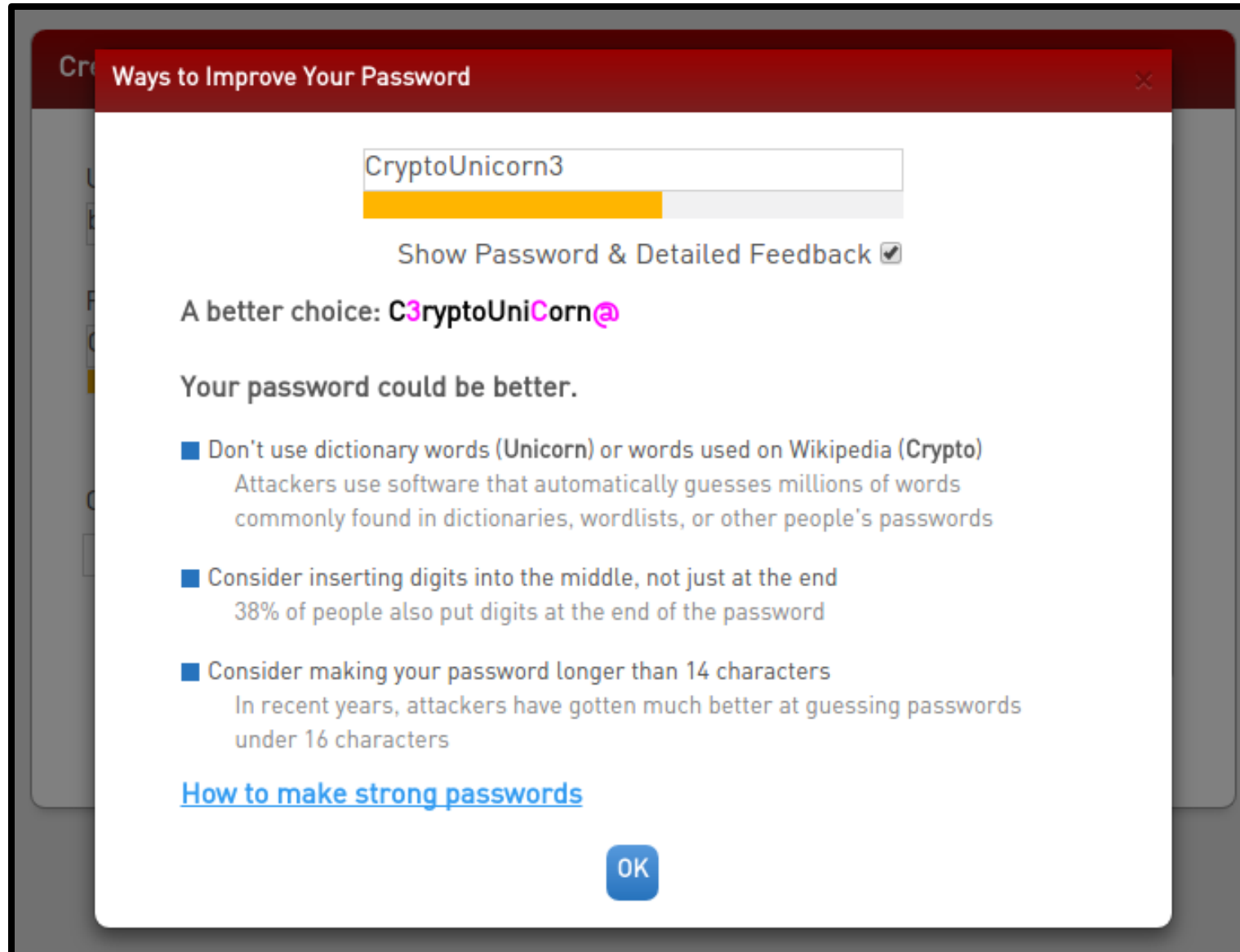
Your password could be better.

- Don't use dictionary words (Unicorn) or words used on Wikipedia (Crypto) [\(Why?\)](#)
- Consider inserting digits into the middle, not just at the end [\(Why?\)](#)
- Consider making your password longer than 14 characters [\(Why?\)](#)

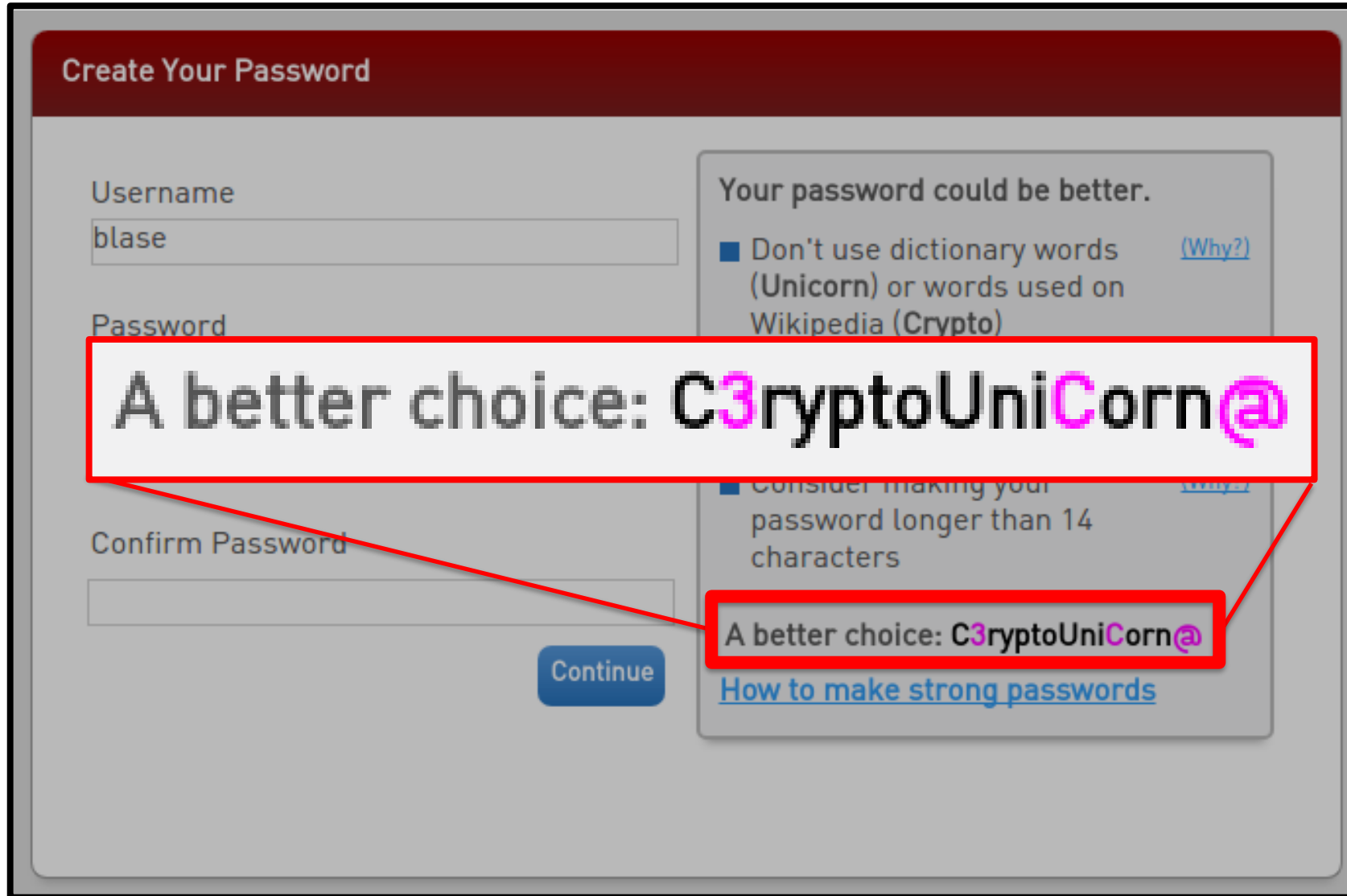
A better choice: C3ryptoUniCorn@

[How to make strong passwords](#)

# Explanations Shown in Modal



# Standard Feedback



The image shows a web form titled "Create Your Password". It includes fields for "Username" (containing "blase"), "Password", and "Confirm Password". A "Continue" button is at the bottom. A feedback box on the right contains the text "Your password could be better." followed by two bullet points: "Don't use dictionary words (Unicorn) or words used on Wikipedia (Crypto)" and "Consider making your password longer than 14 characters". Two red-bordered callout boxes highlight a suggested password: "A better choice: C3ryptoUniCorn@".

Create Your Password

Username  
blase

Password

Confirm Password

Continue

Your password could be better.

- Don't use dictionary words (Unicorn) or words used on Wikipedia (Crypto) [\(Why?\)](#)
- Consider making your password longer than 14 characters [\(Why?\)](#)

A better choice: C3ryptoUniCorn@

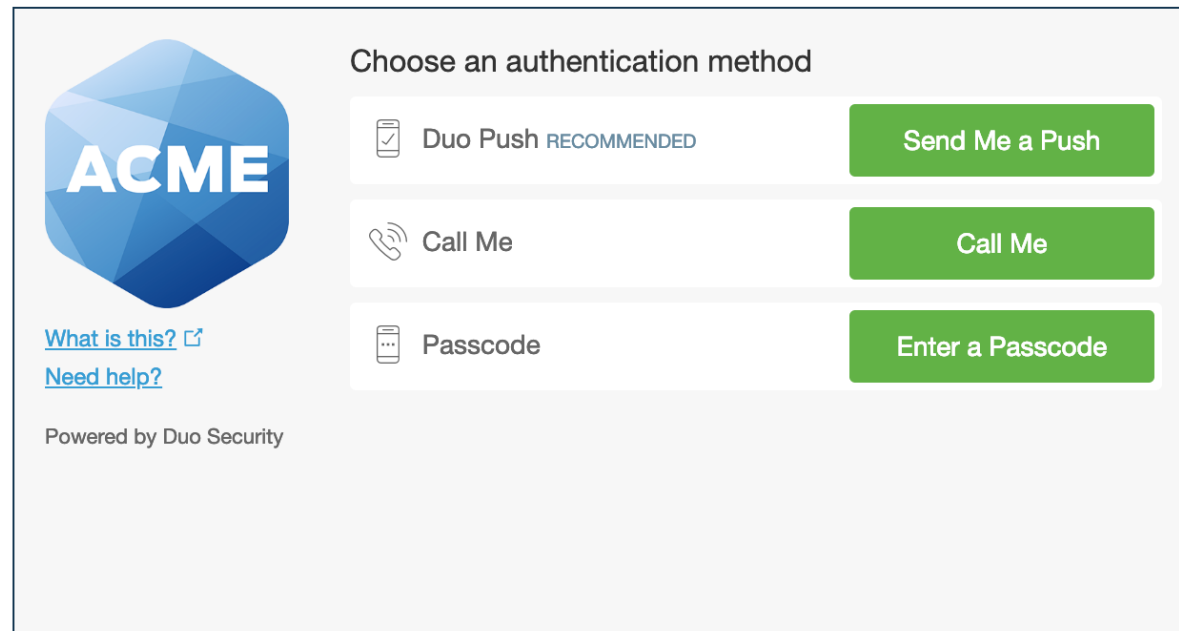
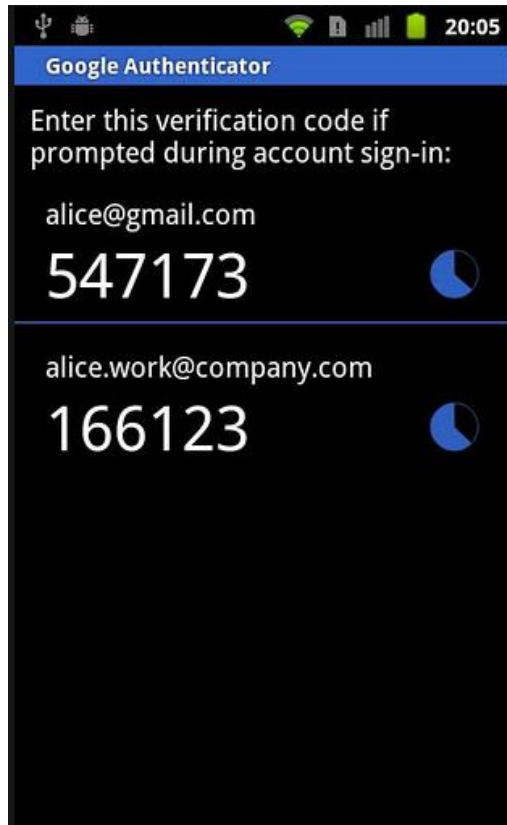
A better choice: C3ryptoUniCorn@

[How to make strong passwords](#)

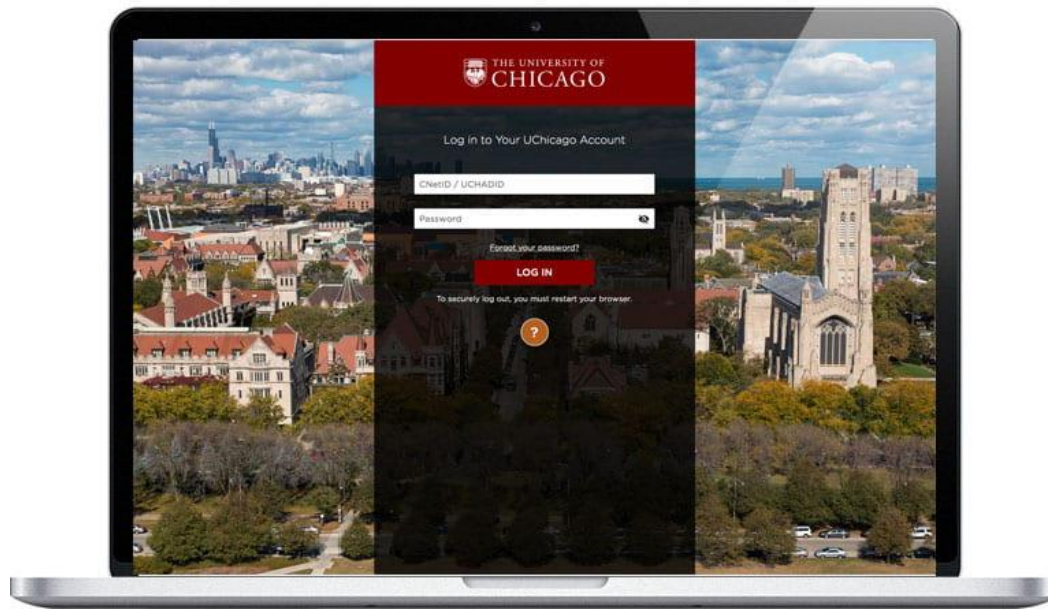


# Authentication in Practice: Password Add-Ons / Alternatives

# Two-Factor Auth



# Single Sign-On



# Single Sign-On: Shibboleth

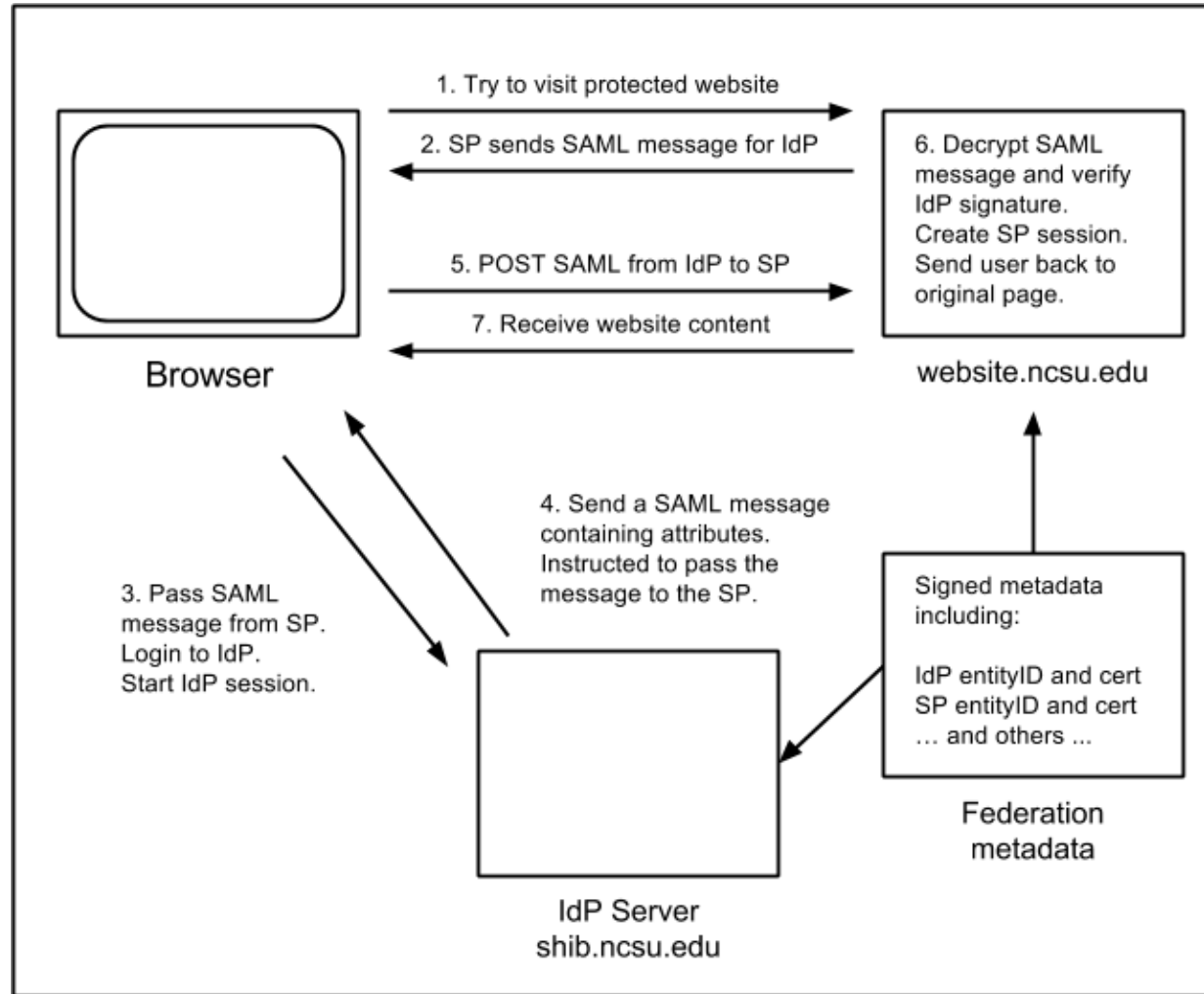


Diagram from <https://docs.shib.ncsu.edu/docs/shibworks.html>

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

Listing

trdealmgm4uvm42g.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

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

Qty: 0

Buy It Now

Favorite Question

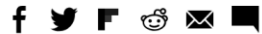
[BEST PRODUCTS](#)[REVIEWS](#)[NEWS](#)[VIDEO](#)[HOW TO](#)[SMART HOME](#)[CARS](#)[DEALS](#)[JOIN / SIGN IN](#)

SECURITY

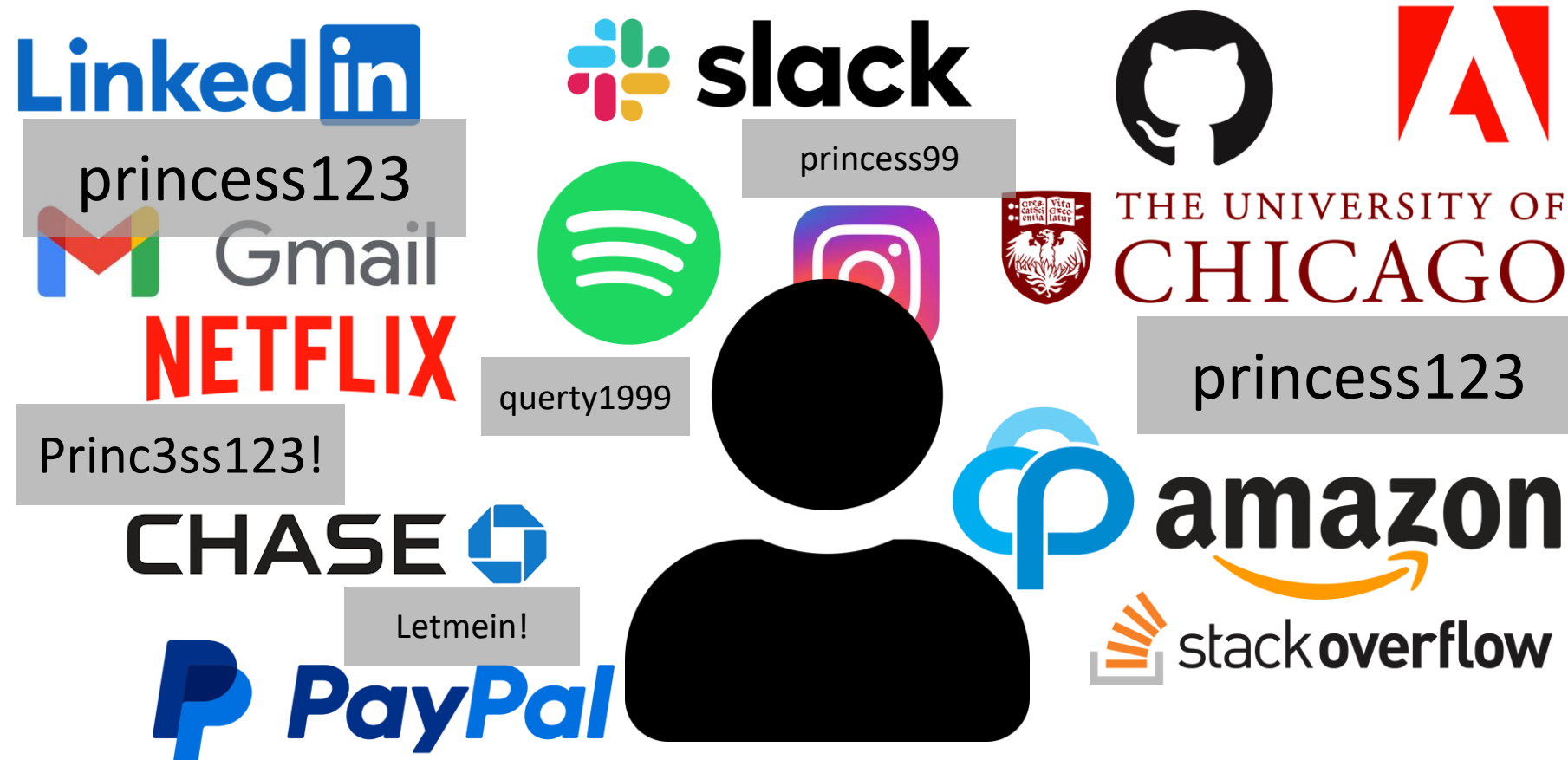
# Facebook buys black market passwords to keep your account safe

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

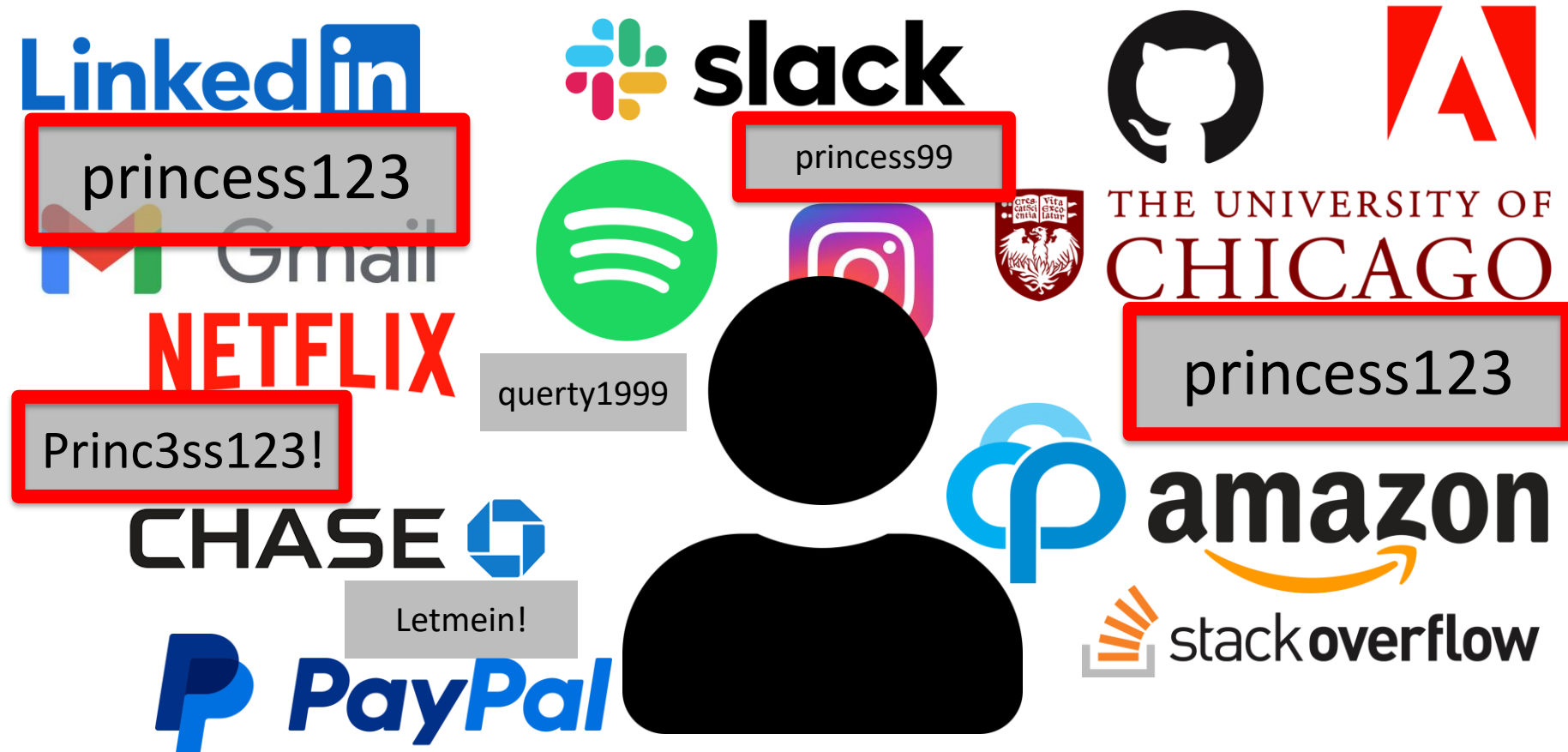


# Measuring Vulnerability to Password Reuse



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

Create Password or Passphrase

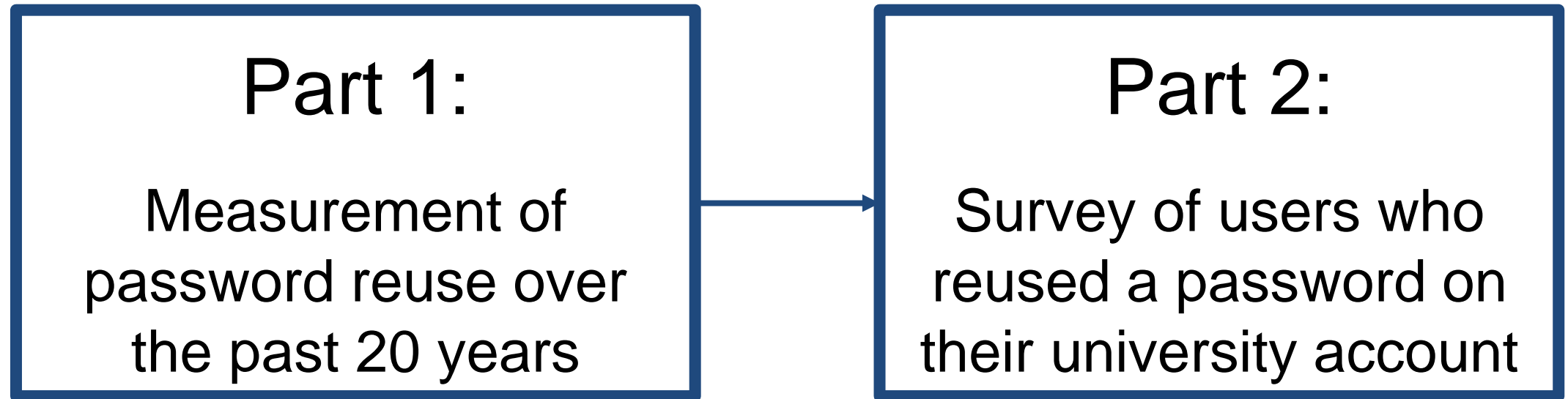
You have already used this password before. Please choose a different one.

# UChicago Password History Database

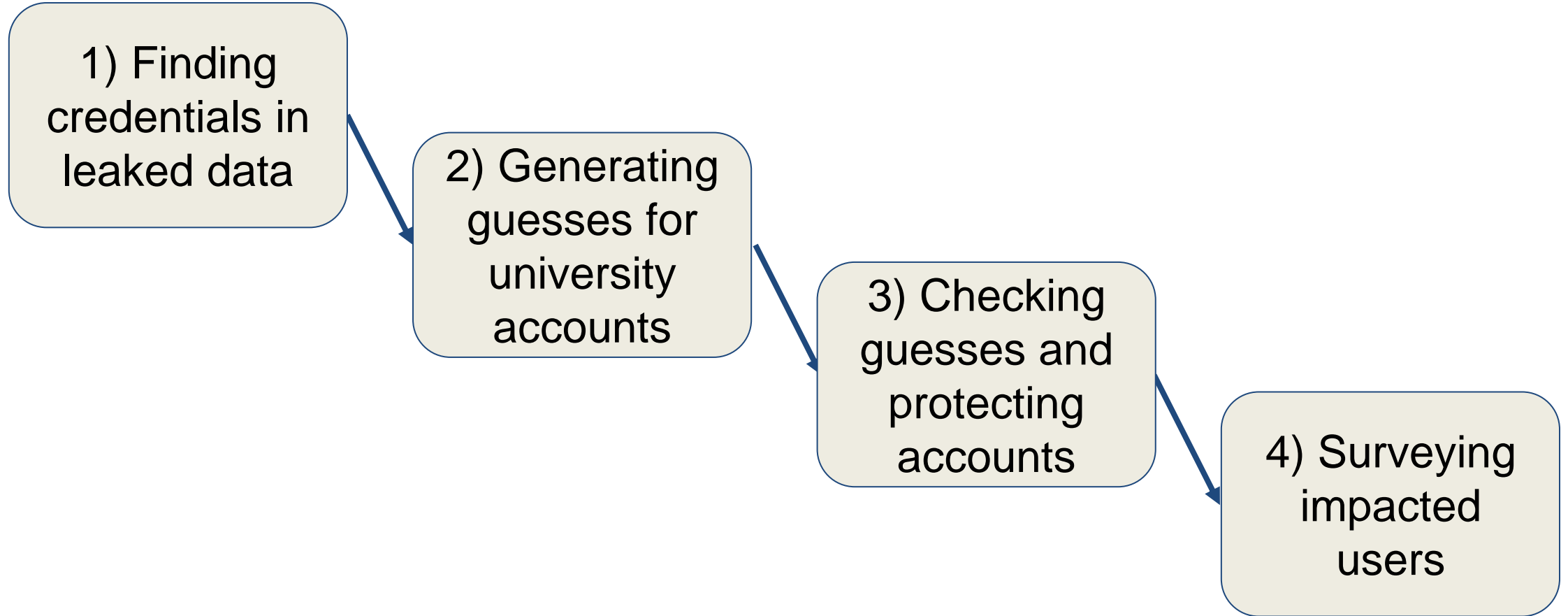
Username	Hash of Password	Created	Changed	
weimf	<b>hash(i&lt;3cats1234)</b>	Sep 17, 2016	Jul 1, 2019	...
weimf	<b>hash(i&lt;3cats2019!)</b>	Jul 1, 2019	present	...
hszym	<b>hash(p@nc@kes99)</b>	Aug 15, 2018	present	...
blase	<b>hash(cyb#rS3curity)</b>	Nov 10, 2017	Aug 23, 2019	...
...	...	...	...	...



# Study Flow



# Study Flow

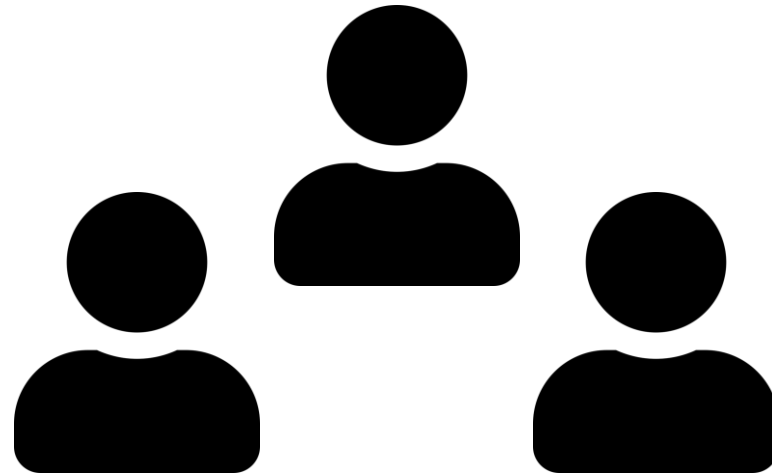


# Study Flow



# 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

Chegg



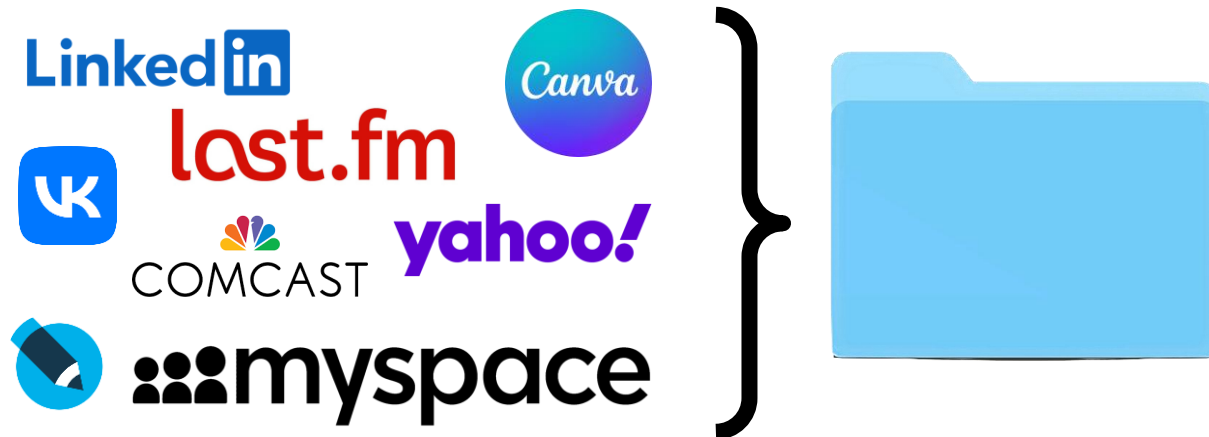
neopets®

wattpad 

# 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**

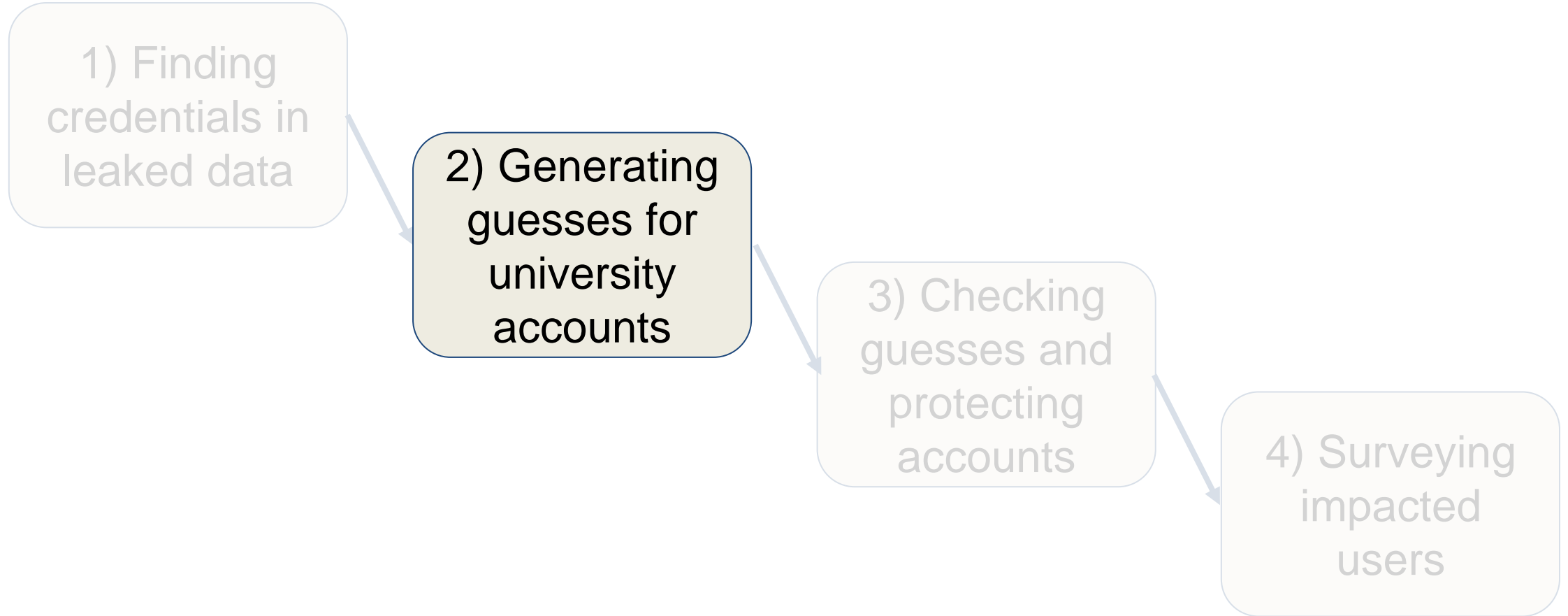


**blase**



**blase99@gmail.com**

# Study Flow





# Compliance With Historical Password Policies

2) Generating guesses for university accounts

	Time Period	Length	Character Classes
<b>Password</b>	2015 - Present	12 - 19	3+
	2010 - 2015	8 - 16	3+
	Prior to 2010	8 - 16	2+
<b>Passphrase</b>	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

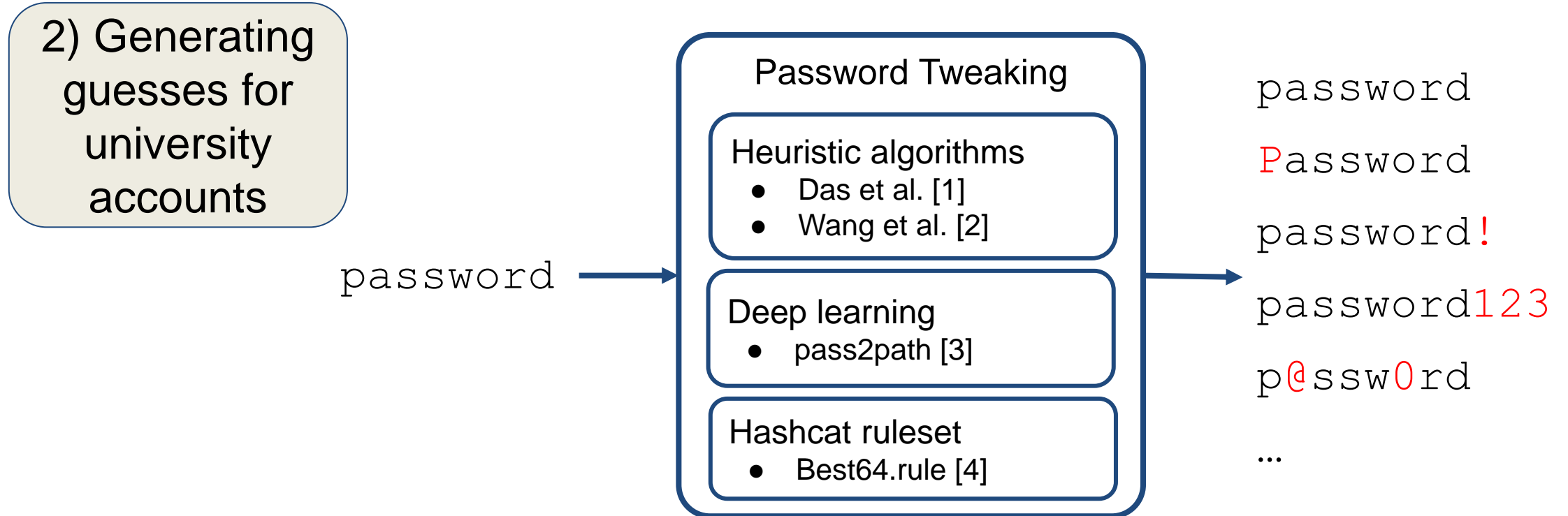


password1 → password1

LinkedIn1 → UChicago1

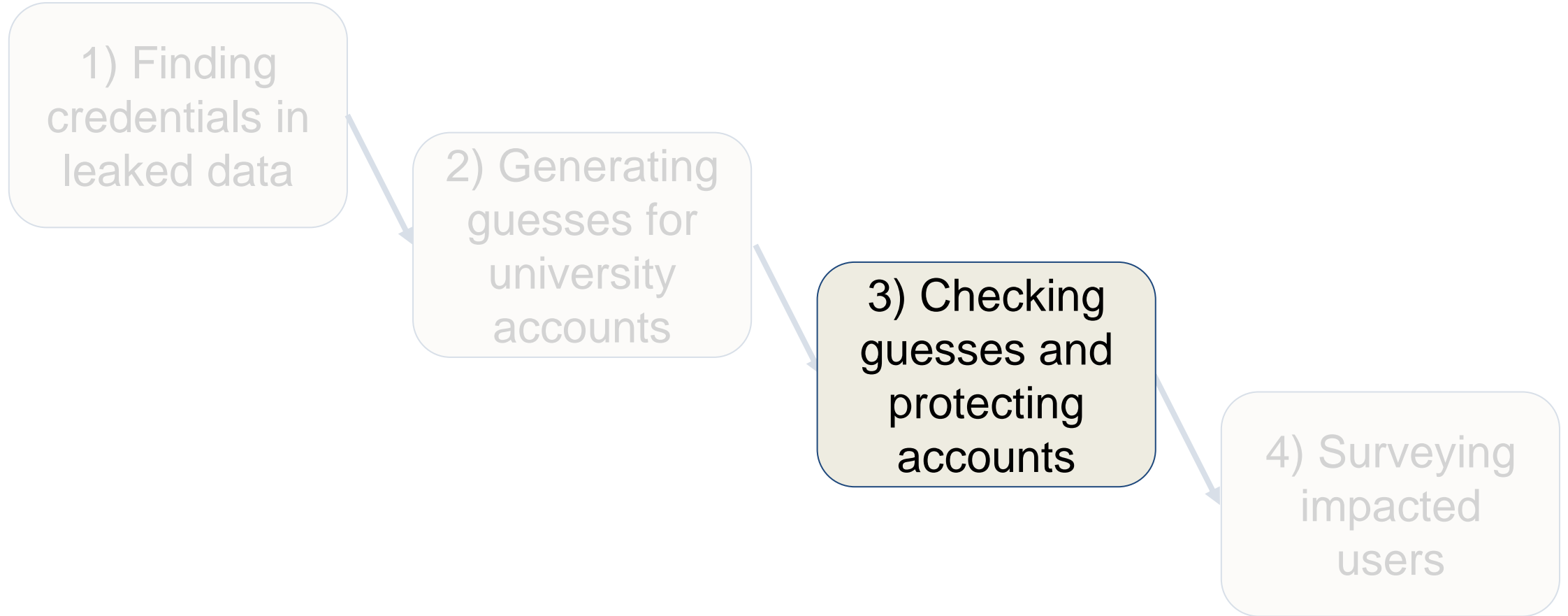
P@ssw0rd1234 → P@ssw0rd1234

# Tweaking Guesses (Similar Passwords)



- [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

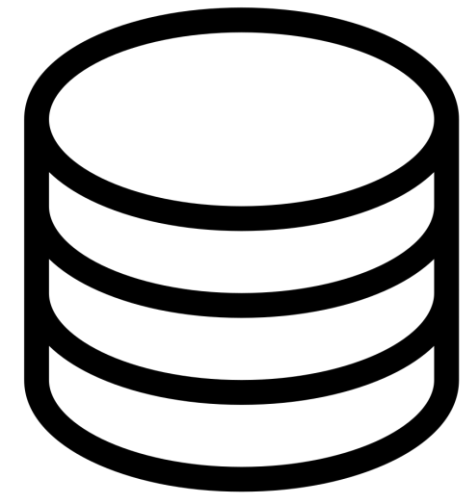


# Transferring Guesses

3) Checking guesses and protecting accounts

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

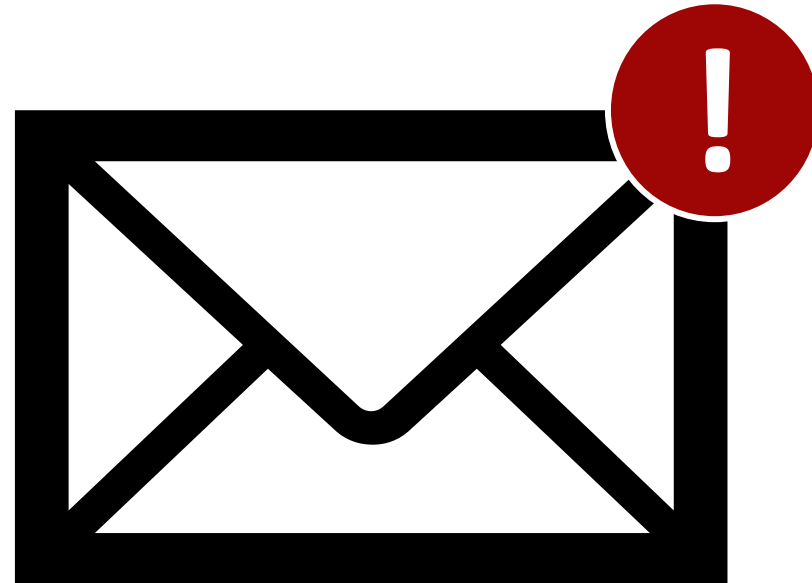
Credential Guesses



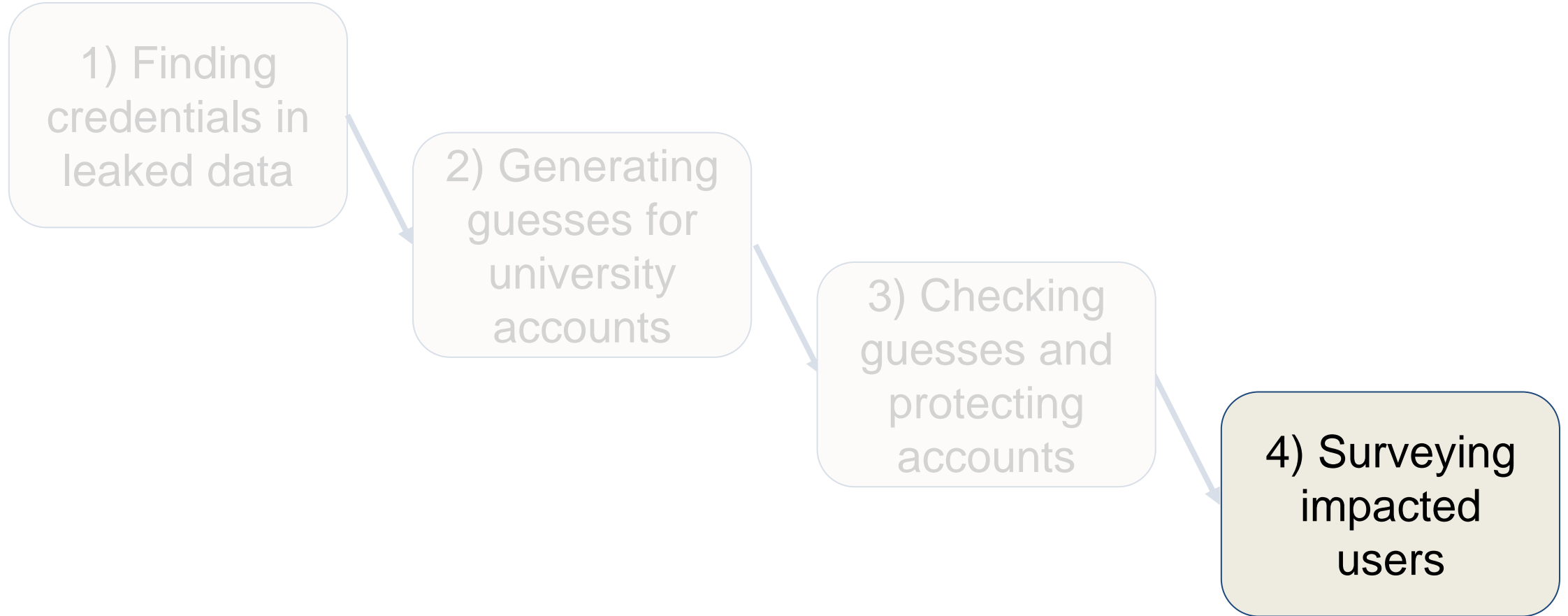
UChicago  
Password History  
Database

# Notifying Vulnerable Users

3) Checking guesses and protecting accounts



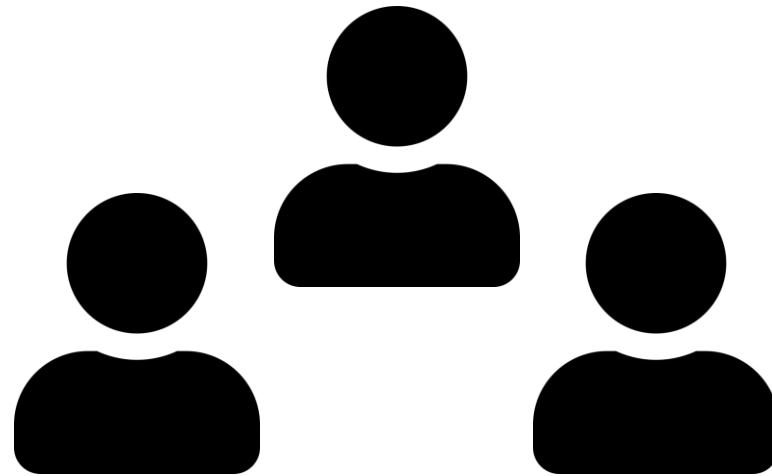
# Study Flow





# 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

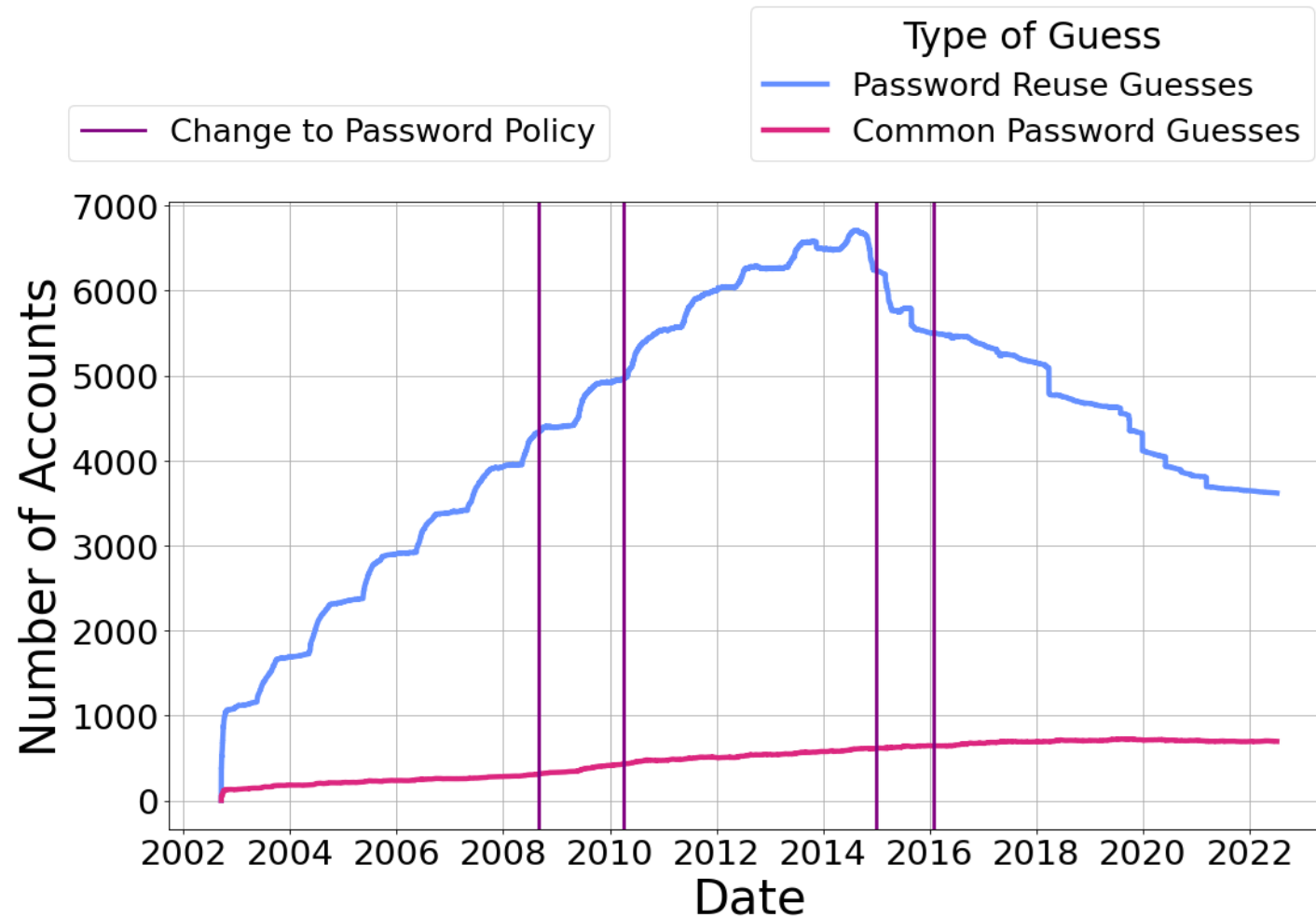
71 individual service breaches



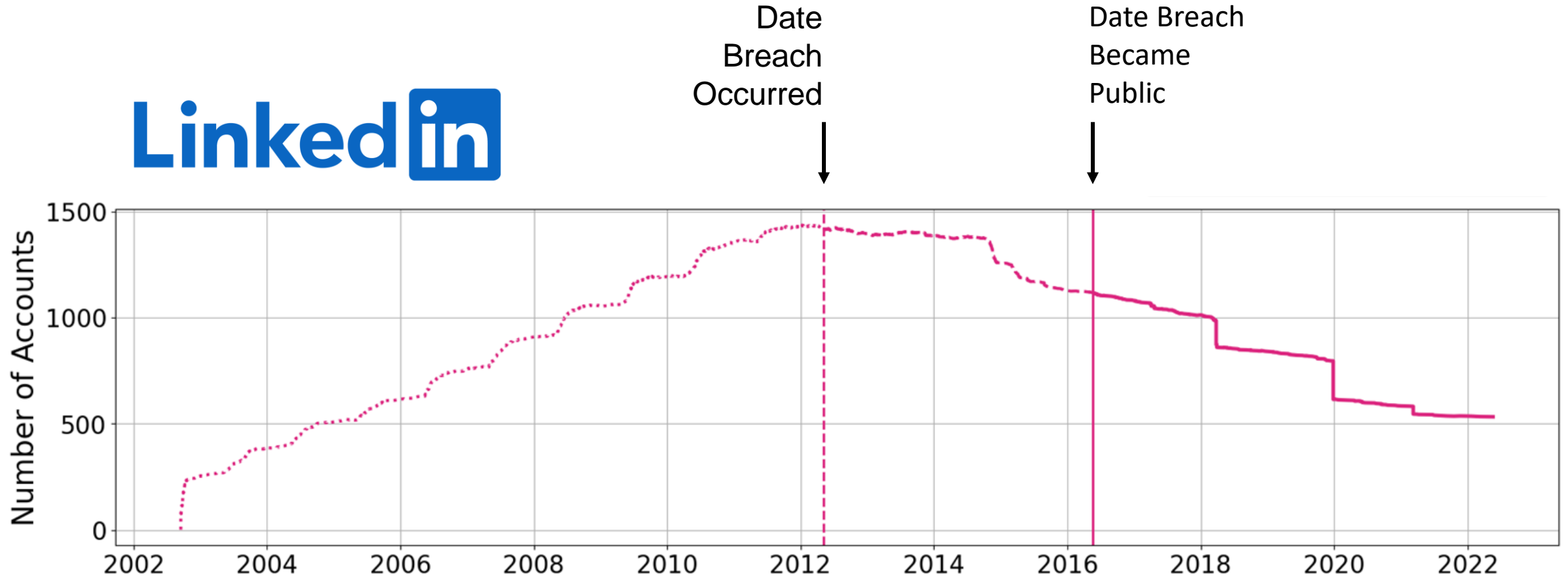
# Sources of Correct Guesses

71 individual service breaches  
...and all 12 breach compilations

# Number of Vulnerable Accounts Over Time

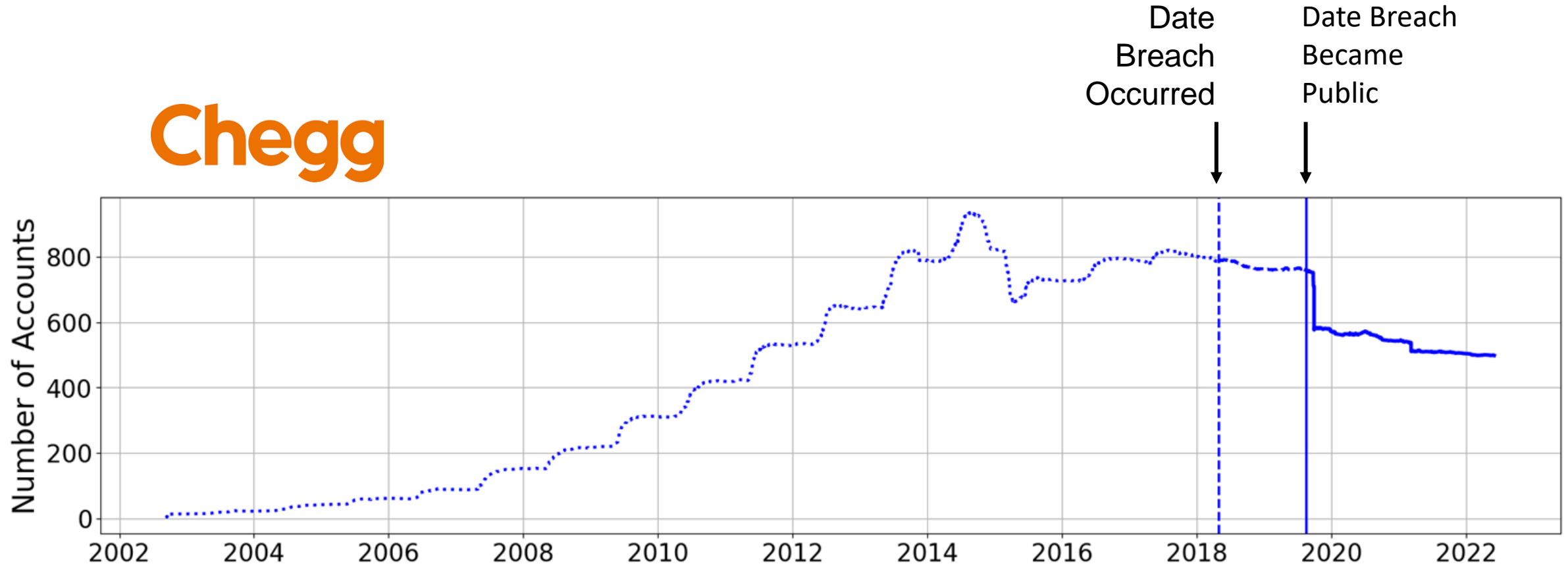


# Some Accounts Remained Vulnerable For Years



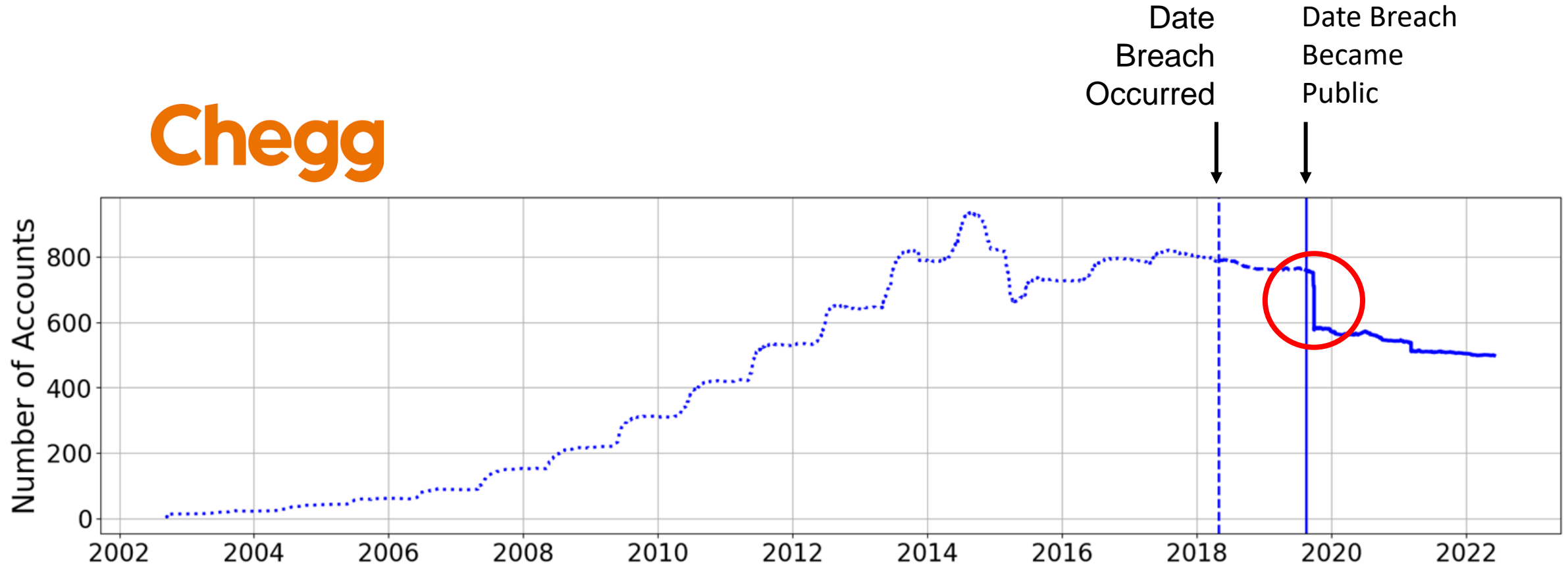
# Some Accounts Were Quickly Exploited

Chegg



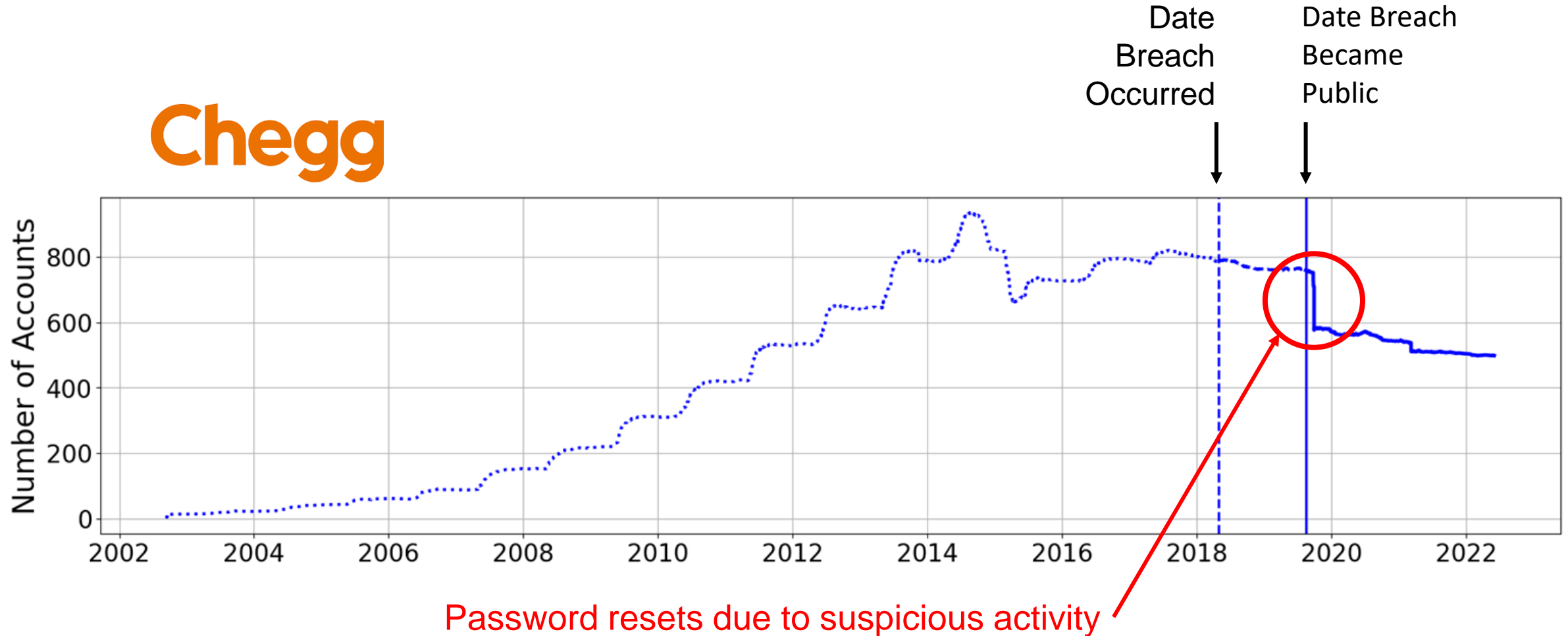
# Some Accounts Were Quickly Exploited

Chegg

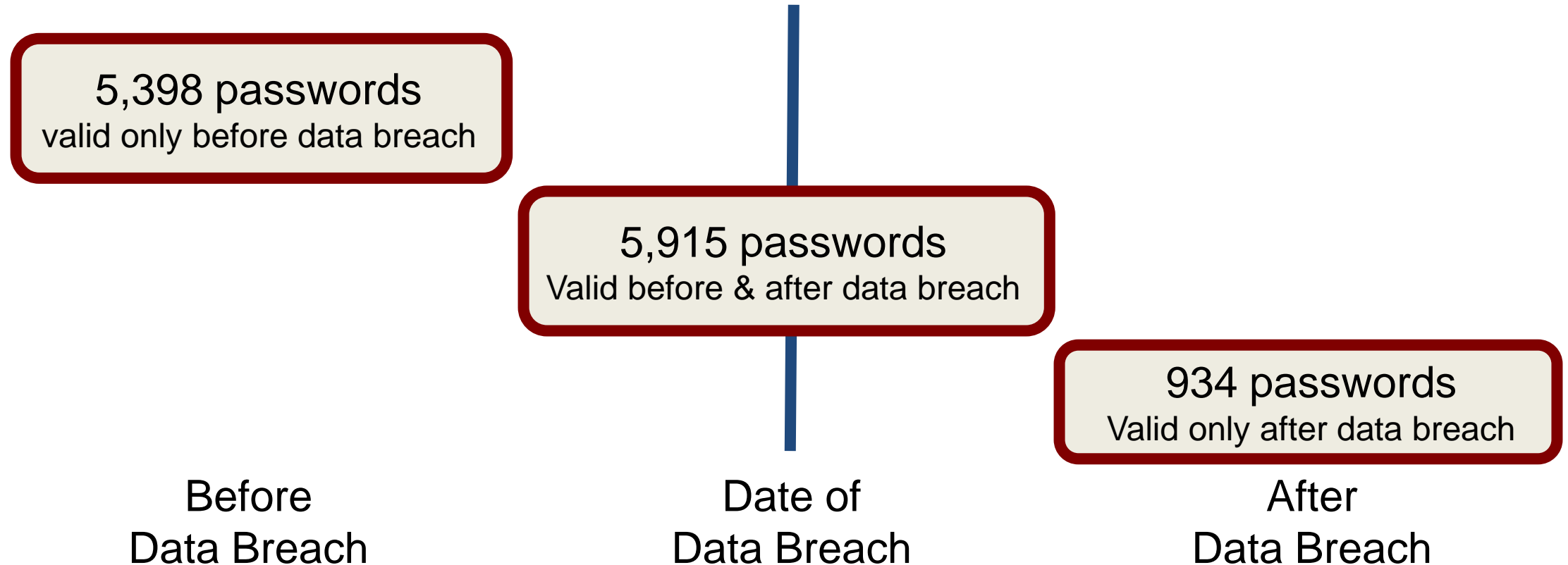


# Some Accounts Were Quickly Exploited

Chegg



# 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

85.3%

Hashed

14.7%

---

Sunshine!  
correctbatteryhorsestaple  
i@mfor3tful!  
ineedapassword

5F4DCC3B5AA765D61D8327DEB882CF99  
482C811DA5D5B4BC6D497FFA98491E38  
62099D23A9D9910879D67449D9E084ED  
1C8F93D67A694EE1DE6363D20228DAC8

# Importance of Tweaking Guesses

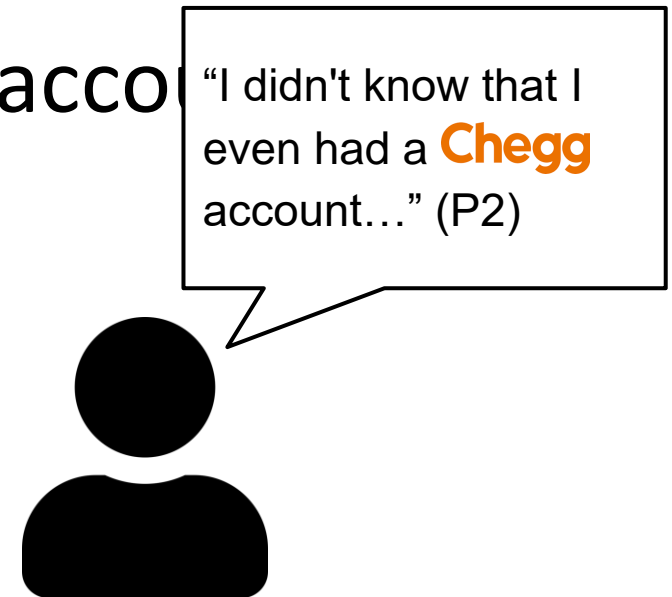
Verbatim  
Reuse  
54.7%

password → `P`assword  
password!  
password123  
p@ssw0rd  
pa\$\$word

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 accounts 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

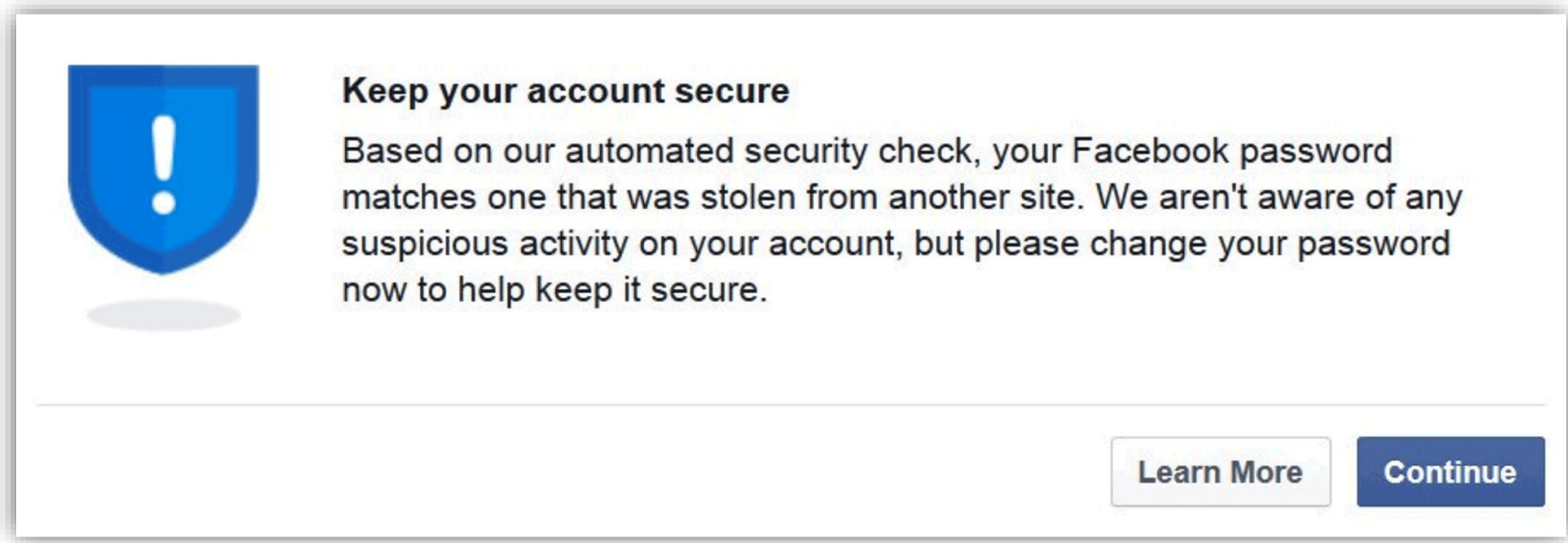


Check for reuse of hashed and tweaked passwords in less common data breaches



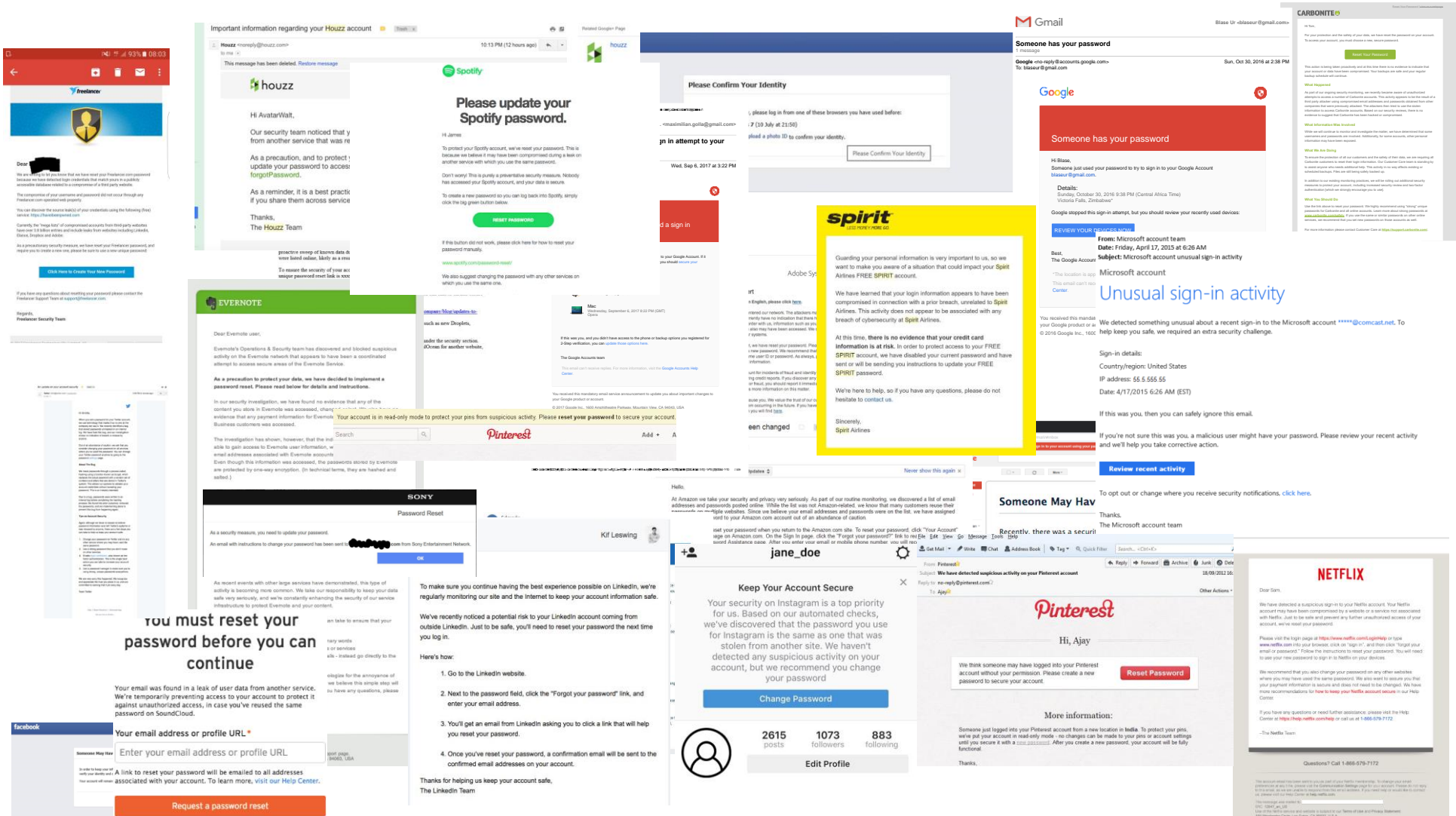
Use 2FA and consider moving to FIDO2 Passwordless Authentication

# 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.

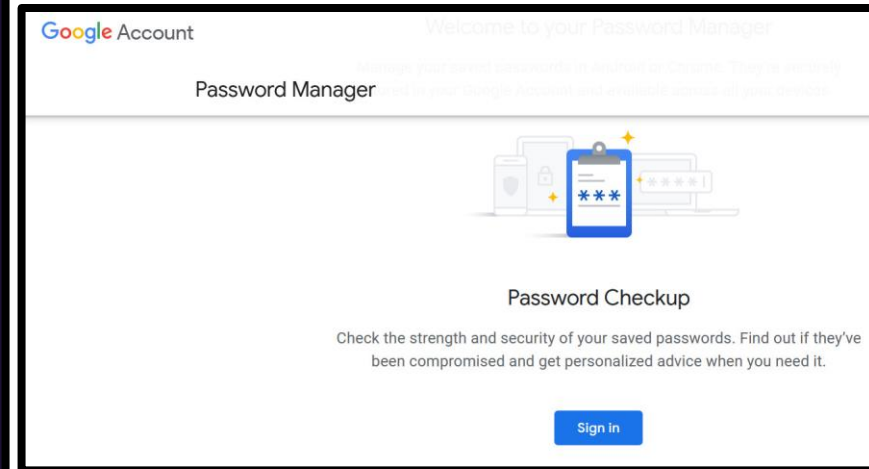
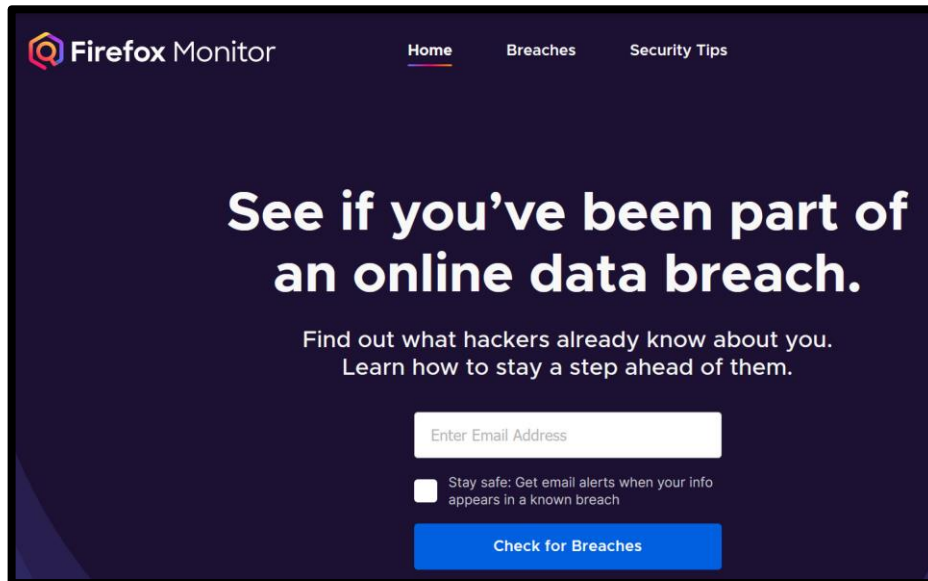
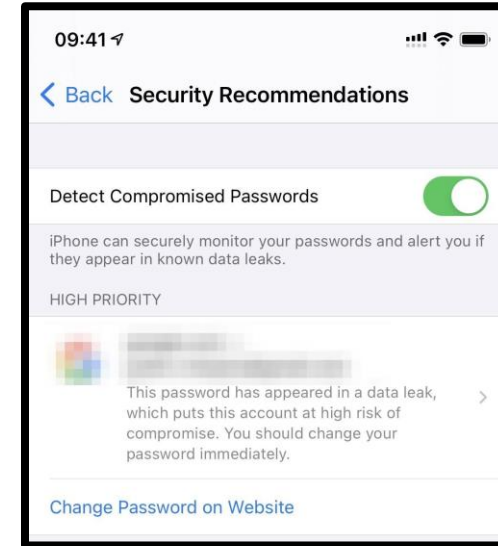
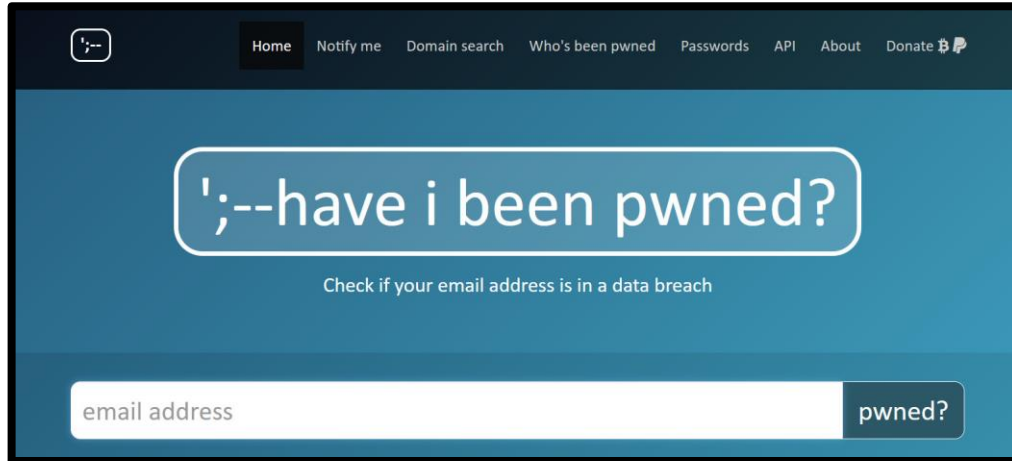
# Password-Reuse Notifications



# Authentication in Practice: Checking for Compromised Credentials



# Checking for Compromised Credentials



# Checking for Compromised Credentials

## Under the hood:

How Password Checkup helps keep your accounts safe

01

Whenever Google discovers a username and password exposed by a data breach, we store a strongly hashed and encrypted copy of the data.



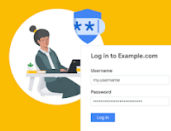
We keep an unencrypted, 2-byte hash prefix to partition the database.



We encrypt the full hash using a secret key known only to Google.

02

When you log in to a site you use, Password Checkup will send a strongly hashed and encrypted copy of your username and password to Google. This ensures that Google never learns your account details.



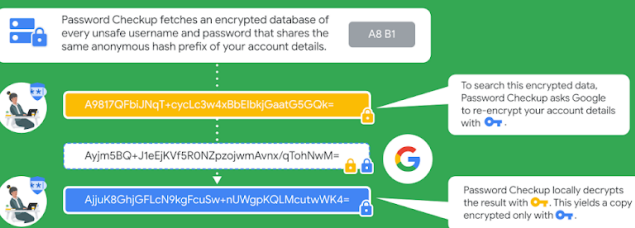
Google only learns an anonymous hash prefix of your account details.



Password Checkup encrypts your full account details using a secret key known only to you.

03

We use **private set intersection** with **blinding** to search through every unsafe username and password without revealing your account details, or anyone else's, during the process.



04

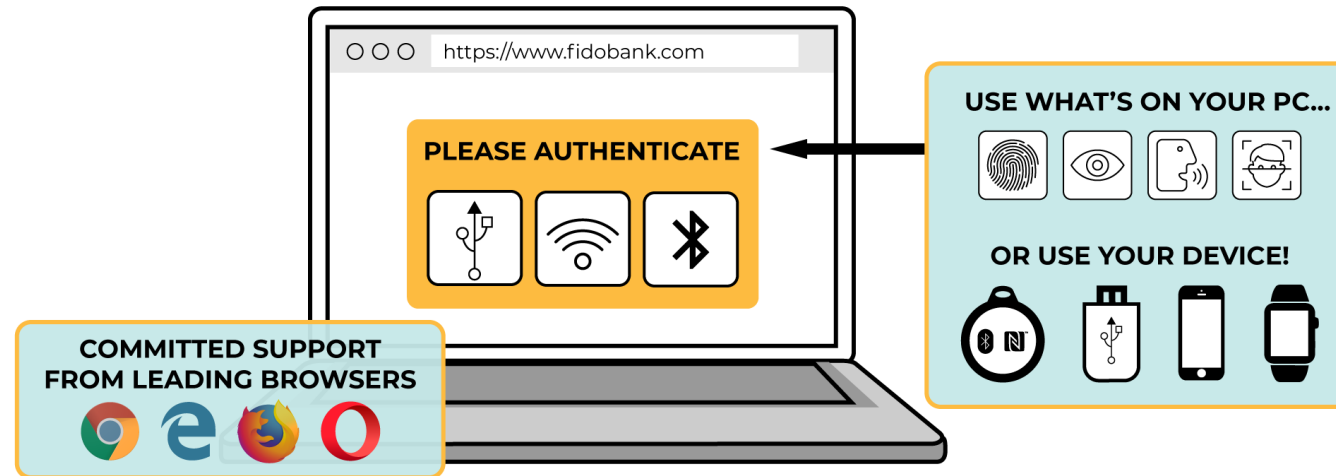
The final check for whether your username or password was in a data breach is entirely local. If your account details were exposed, you should change your password immediately.



# Authentication in Practice: Moving Towards A Passwordless World?

# Passwordless FIDO2

## FIDO2 BRINGS SIMPLER, STRONGER AUTHENTICATION TO WEB BROWSERS



## FIDO AUTHENTICATION: THE NEW GOLD STANDARD



Protects against phishing, man-in-the-middle and attacks using stolen credentials



Log in with a single gesture – HASSLE FREE!

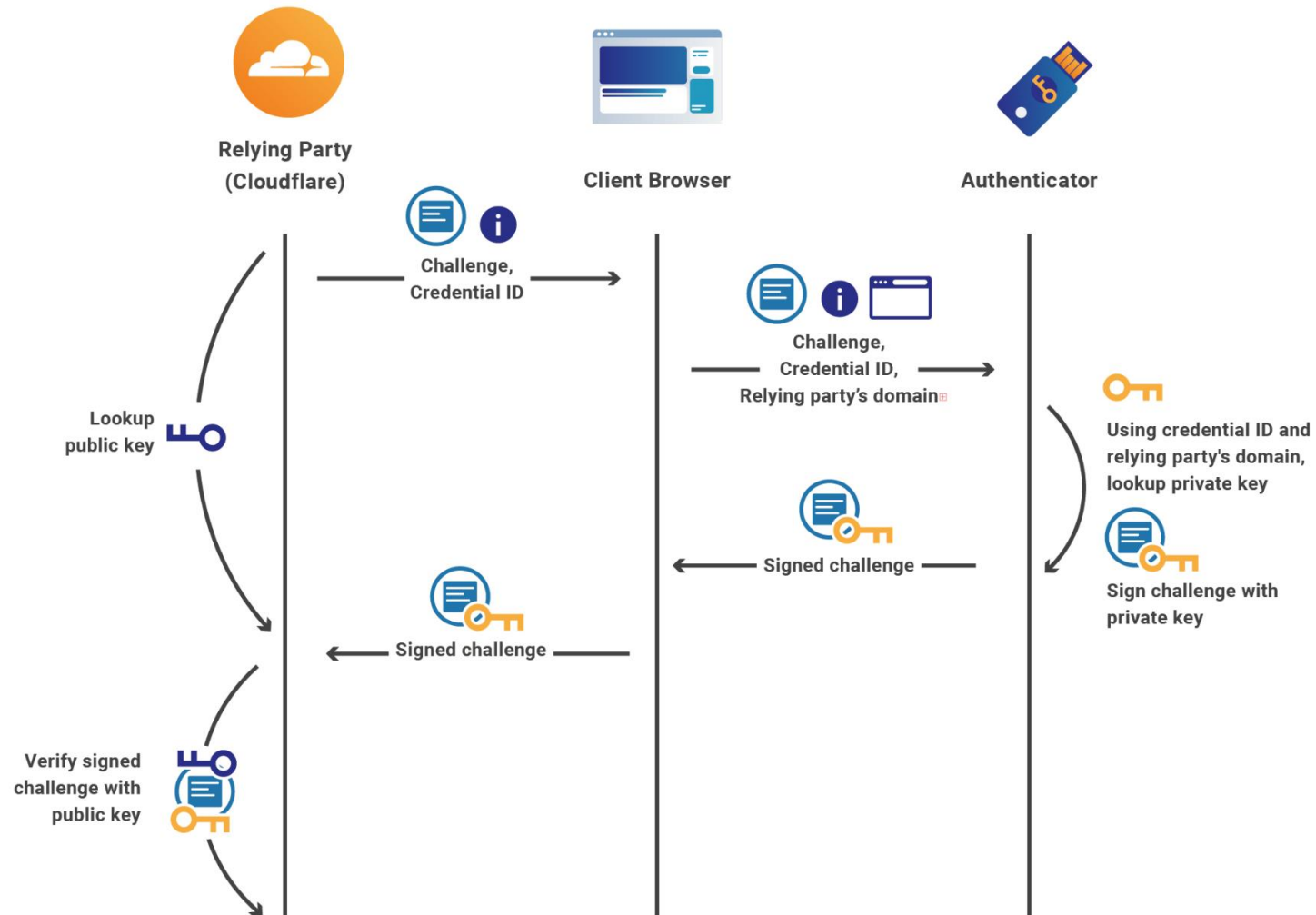


Already supported in market by top online services

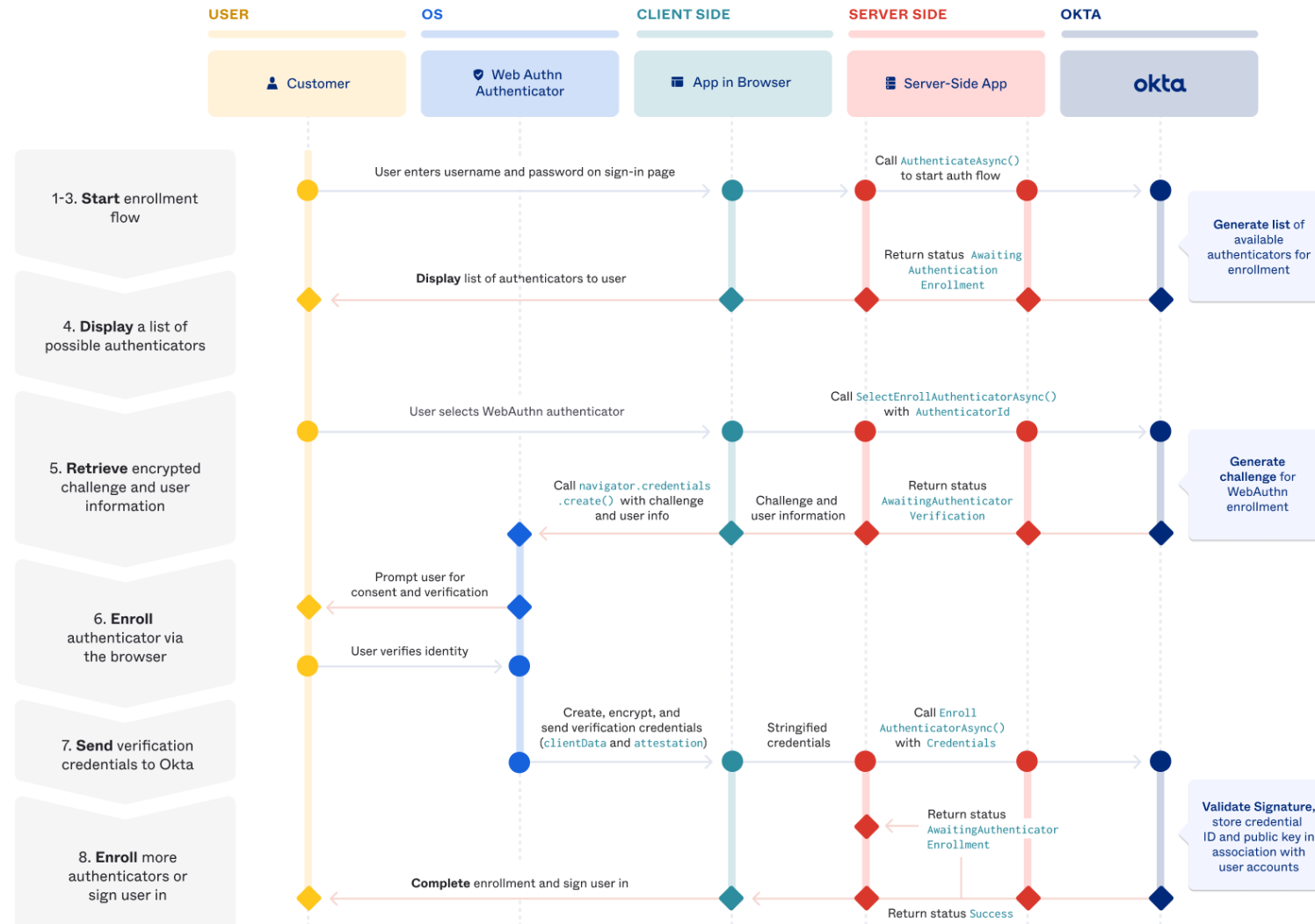
# Passwordless FIDO2

- 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



# Integrating WebAuthn With Okta



# 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:

## Our Passwordless journey

Passkeys bring us much closer to the passwordless future we've been mapping out for over a decade.

2008	2011	2012	2013	2014	2017	2019	2023
Launched Google Password Manager for easier and safer sign-ins.	Enabled 2-Step Verification (2SV) for Google accounts.	Introduced phishing-resistant security key for Google employees.	Joined the FIDO Alliance to drive open standards for a passwordless world.	Expanded phishing-resistant security keys for everyone.	Introduced Advanced Protection Program (APP) for high-risk users.	Extended our FIDO support in Android for passwordless re-auth across websites.	Enabled passkeys for Google Accounts, Workspace customers and 3rd party partners on Chrome and Android.

What about  
Biometrics?

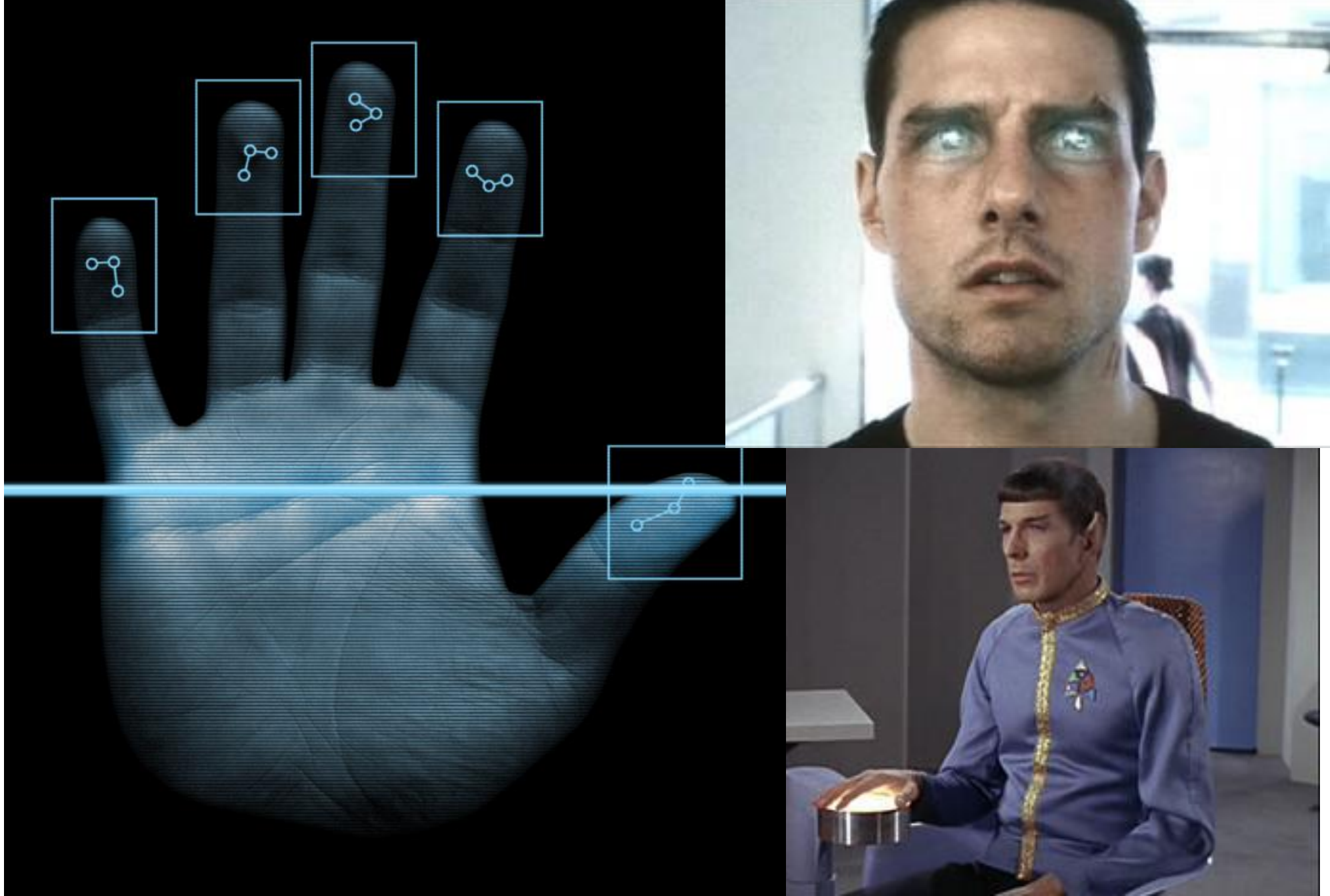


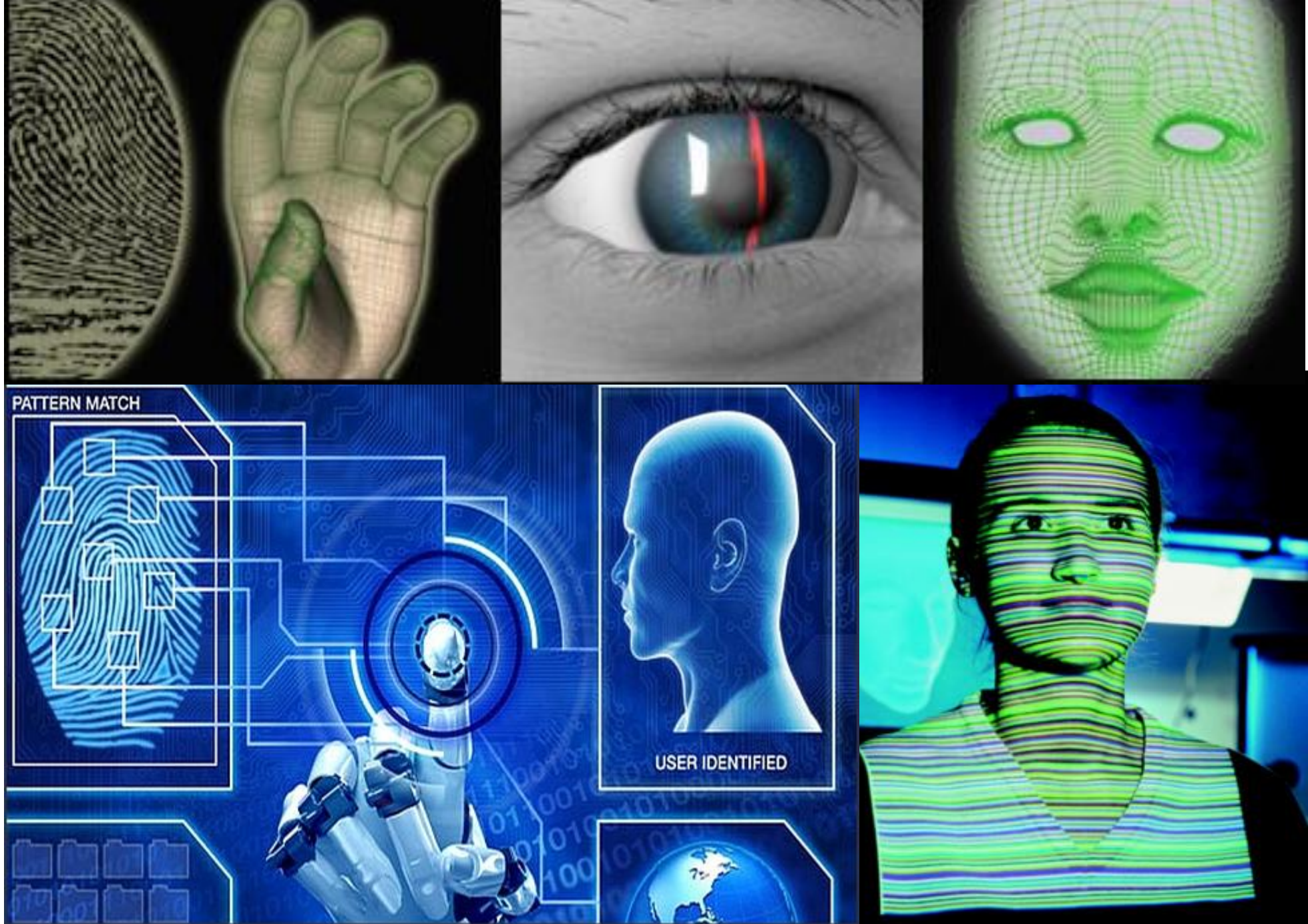
•Images on previous slide fair use from androidcentral.com and businessinsider.com. Photo above fair use from abcnews.com



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







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



# Biometrics

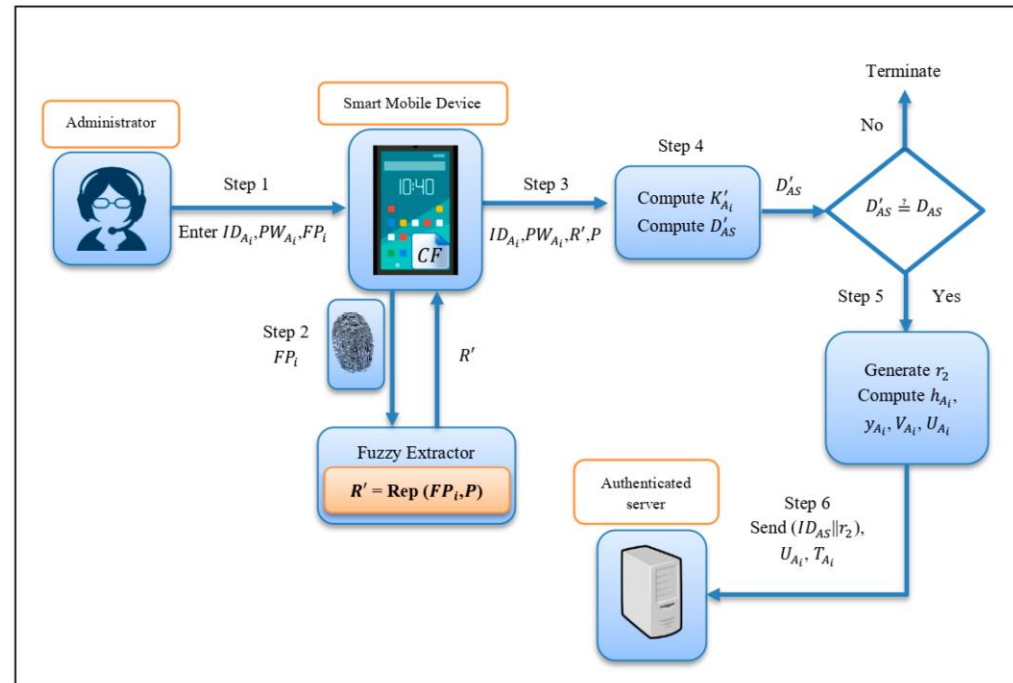
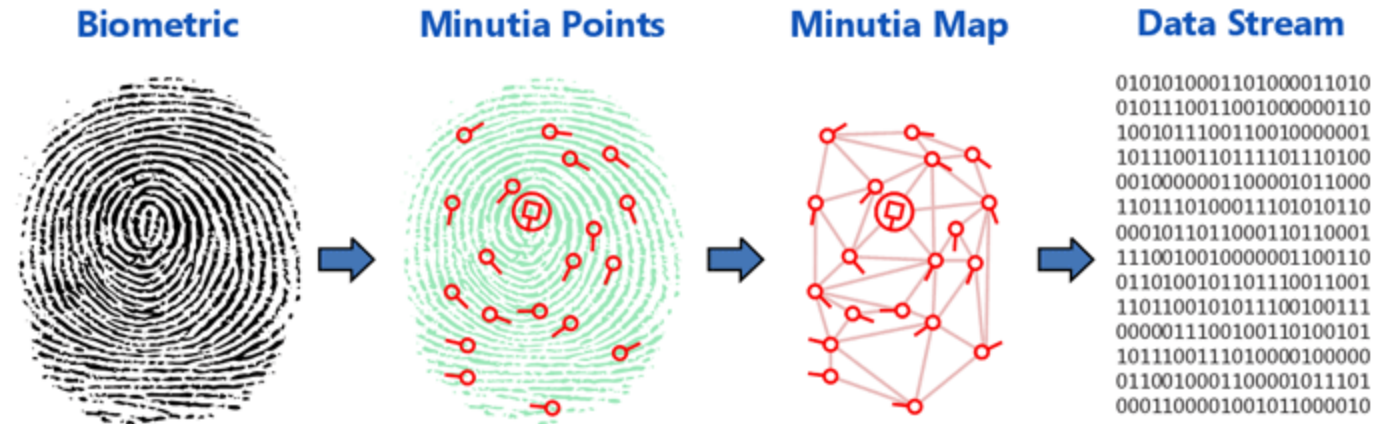
- Fingerprint
- Iris scans or retina scans
- Face recognition
- Finger/hand geometry
- Voice or speech recognition
- The way you type
- (Many others)

# 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

