



Reused Password

This password is used for more than one of your items. Change your password to something unique.

Change password on website

Ignore



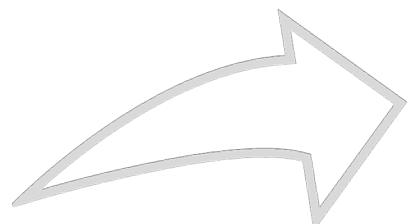
University of Chicago

Measuring the Risk Password Reuse Poses for a University

Alexandra Nisenoff, Maximilian Golla, Miranda Wei, Juliette Hainline, Hayley Szymanek, Annika Braun, Annika Hildebrandt, Blair Christensen, David Langenberg, and Blase Ur.

Passwords Are Everywhere

- Accounts: 24 -> 100+
- Passwords: 6-8



Memorability Issues

Coping

Memorable
Passwords

“Baseball”

Reusing
Passwords

amazon Baseball20
facebook Baseball1!
Google Baseball25



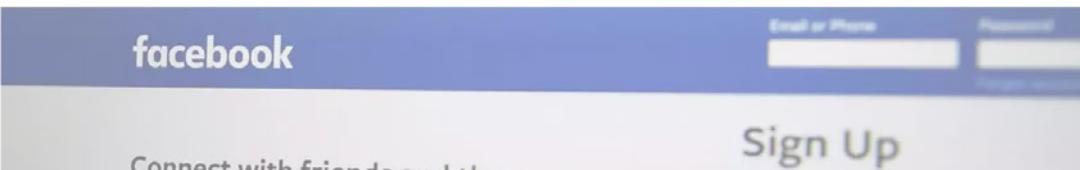
SO, UH, THAT BILLION-ACCOUNT YAHOO BREACH WAS ACTUALLY 3 BILLION

Anatomy of
Adobe's giant

Facebook

Facebook says it
had personal info
of 928 million users
recently breached.

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



ars TECHNICA — BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

RISK ASSESSMENT — How LinkedIn's password sloppiness hurts us all

Have I Been Pwned

17,294,130,092

pwned accounts



You Can Now Look Up Your Terrible 2006 MySpace Password

June 29, 2016 // 11:35 AM EST



Written by
LORENZO FRANCESCHI-BICCHIERAI
STAFF WRITER



Password Reuse

Speed-running identity theft.

Reuse Attacks?



Email	SHA-1 Hash
jenny@gmail.com	aef7e39e...
joe@mail.com	5820c4ee...
john@hotmail.com	36c50933...
...	...



Reuse Attacks?

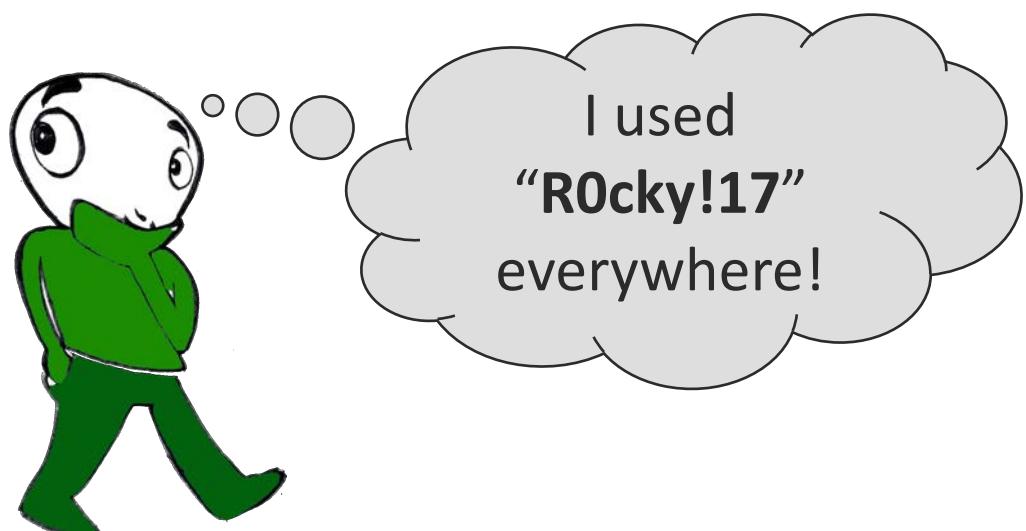
Email	Cracked SHA-1
jenny@gmail.com	Hiking91
joe@mail.com	R0cky!17
john@hotmail.com	I Love Bananas!
...	...



Reuse Attacks?



Email	Cracked SHA-1
jenny@gmail.com	Hiking91
joe@mail.com	R0cky!17
john@hotmail.com	I Love Bananas!
...	...



Reuse Attacks?



Email	Cracked SHA-1
jenny@gmail.com	Hiking91
joe@mail.com	R0cky!17
john@hotmail.com	I Love Bananas!
...	...



AcmeCo

Email	Secure Argon2i Hash
joe@mail.com	\$argon2i\$v=19\$m=4096
...	...

Reuse Attacks?

Email	Cracked SHA-1
jenny@gmail.com	Hiking91
joe@mail.com	R0cky!17
john@hotmail.com	I Love Bananas!
...	...



Let's match the
email address



AcmeCo

Email	Secure Argon2i Hash
joe@mail.com	\$argon2i\$v=19\$m=4096,p=1,t=1\$...\$...
...	...



Reuse Attacks?



Email	Cracked SHA-1
jenny@gmail.com	Hiking91
joe@mail.com	R0cky!17
john@hotmail.com	ILoveBananas!
...	...



I will try
“R0cky!17”
first!



AcmeCo

Email	Secure Argon2i Hash
joe@mail.com	\$argon2i\$v=19\$m=4096 , ...
...	...

Reuse Attacks?



Email	Cracked SHA-1
jenny@gmail.com	Hiking91
joe@mail.com	R0cky!17
john@hotmail.com	I Love Bananas!
...	...

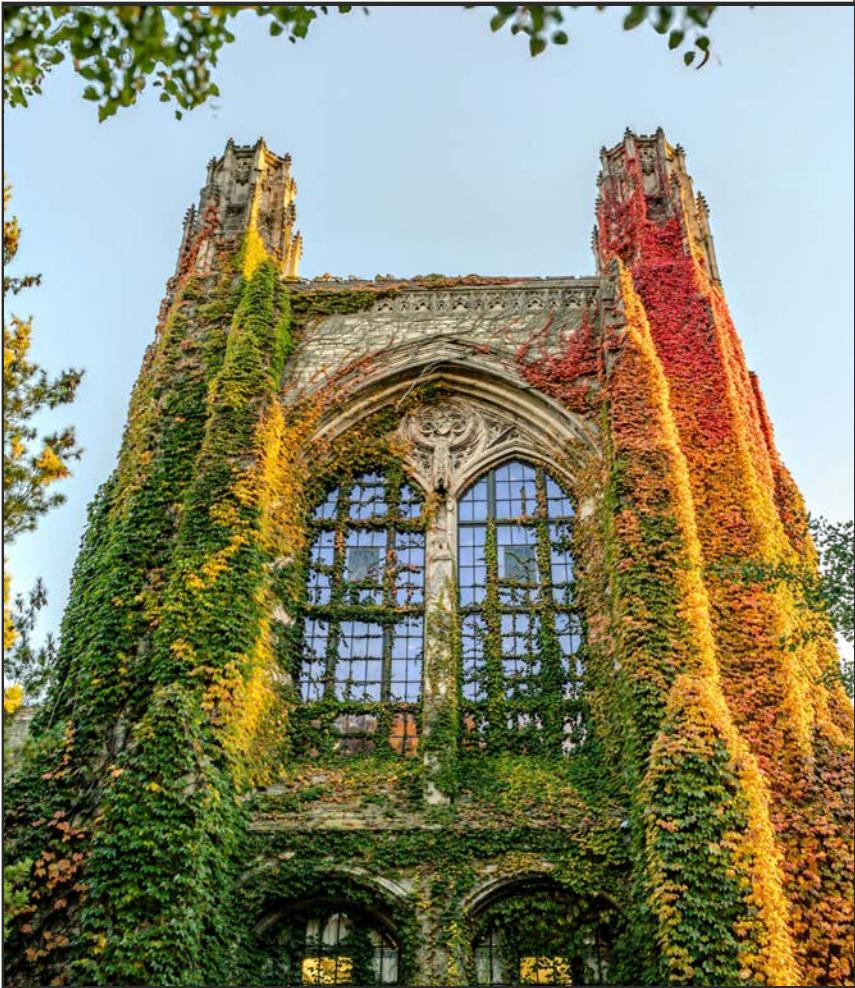


1x guess was enough!



AcmeCo

Email	Cracked Argon2i
joe@mail.com	R0cky!17
...	...



The University of Chicago

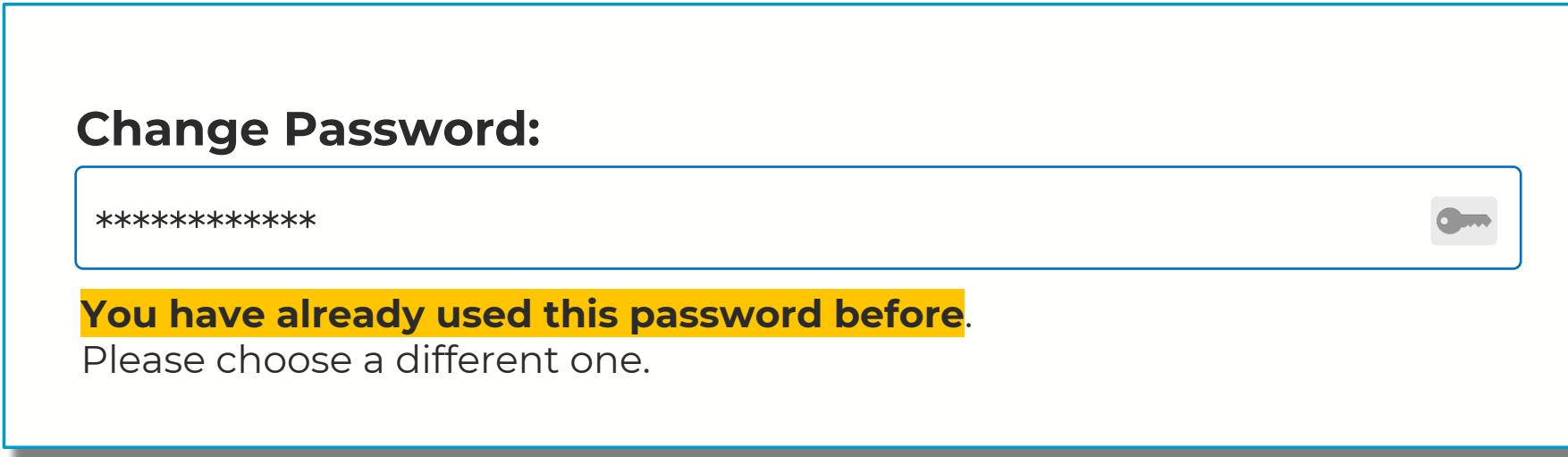
*Let knowledge grow from more to more;
and so be human life enriched.*



University of Chicago



“You have already used this password before.”



UChicago Password History Database

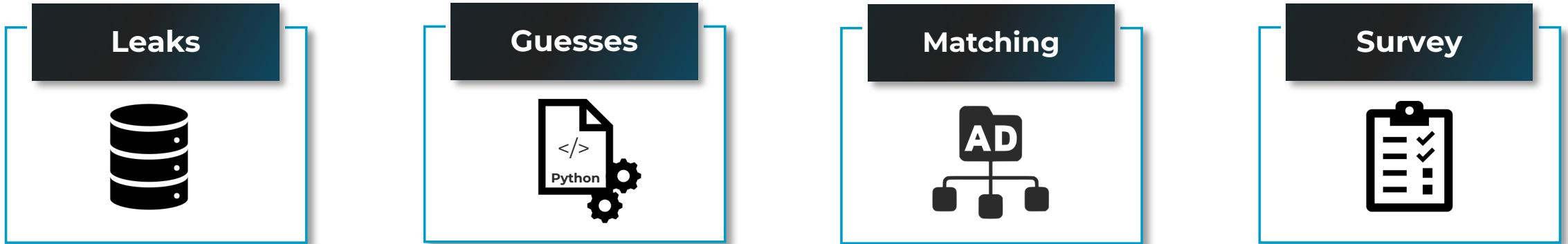
Username	Hash of Password	Created	Changed	
mwei	hash(i<3cats1234)	Sep 17, 2016	Jul 1, 2021	...
mwei	hash(i<3cats2019!)	Jul 1, 2021	present	...
mgolla	hash(p@nc@kes99)	Jun 15, 2017	present	...
jhainline	hash(Tiwchnt89)	Nov 10, 2017	Aug 23, 2020	...
...

A black arrow points from the 'Username' column of the table to the email address 'mgolla@uchicago.edu' located below the table.

A blue curly brace on the right side of the table spans vertically from the bottom row to the top row, covering all five columns. To the right of the brace, the text '20 Years' is written vertically.

mgolla@uchicago.edu

The Idea



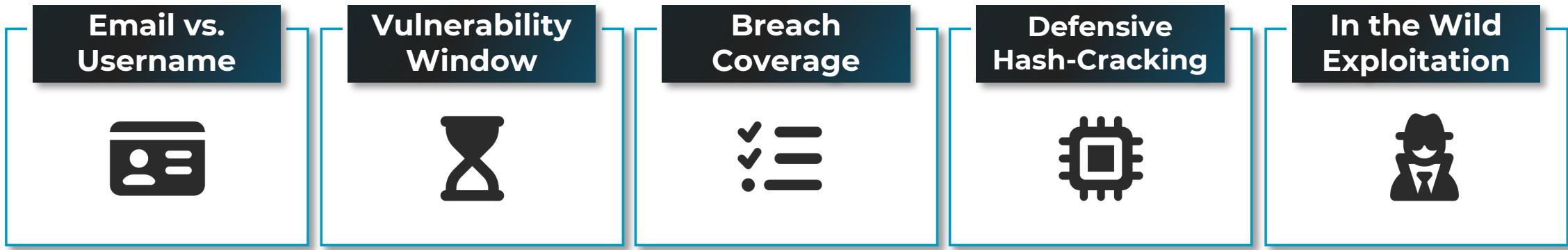
Part 1

Measurement of password reuse over the past 20 years

Part 2

Survey of users that reused a password on their university account

Research Questions



Help Cracking Hashes:

CynoSure Prime and friends, especially Sein Coray (**s3in!c**), Sam Croley (**Chick3nman**), Paul D. Ouderkirk (**pdo**), Robert Reif (**winxp5421**), Michael Sprecher (**hops**), and Royce Williams (**TychoTithonus**).



Blase
Ur



Security, Usability, & Privacy Education & Research



Alexandra
Nisenoff



Maximilian
Golla



Miranda
Wei

... and **Juliette** Hainline, **Hayley** Szymanek, **Annika** Braun,
Annika Hildebrandt, **Blair** Christensen, and **David** Langenberg.

6 Years Later

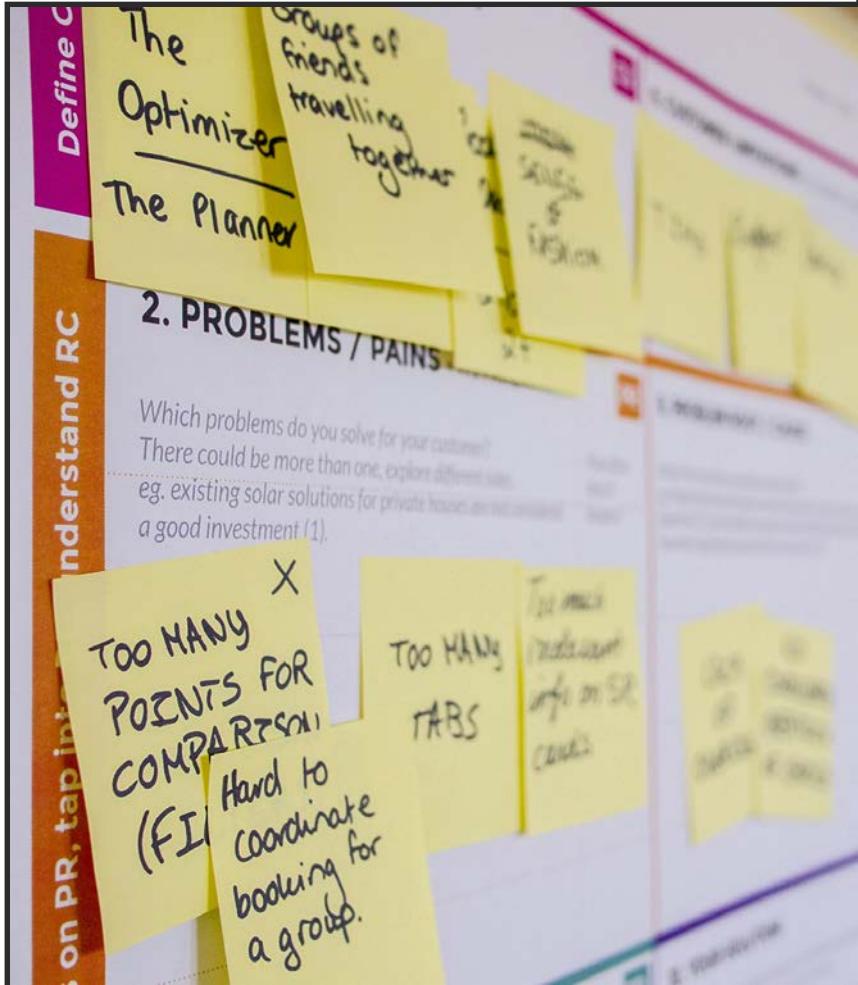
- **Research and Technical Teams**

- Researchers
- IT Services Team (ITS)
- Institutional Review Board (IRB) + Director of the IRB

- **Leadership and Administrative Bodies**

- General Counsel (Chief Legal Officer)
- Provost's Office (Chief Academic Officer)
- IT Leadership (Chief Information Officer)
- Communications Team
- Administration
- Alumni Association





Method

The part of the paper where you pretend you knew what you were doing the whole time.

Hospital + Alumni

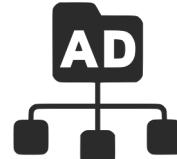
Leaks



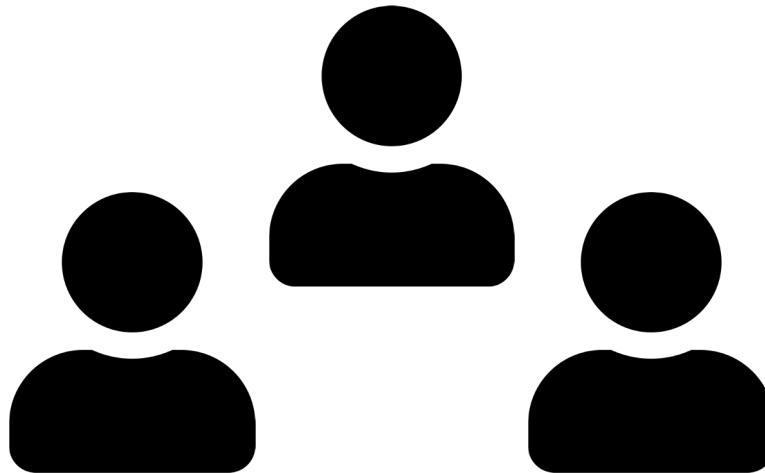
Guesses



Matching



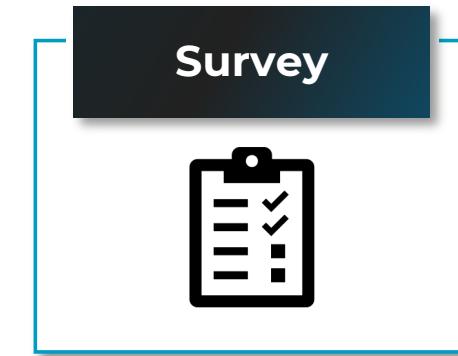
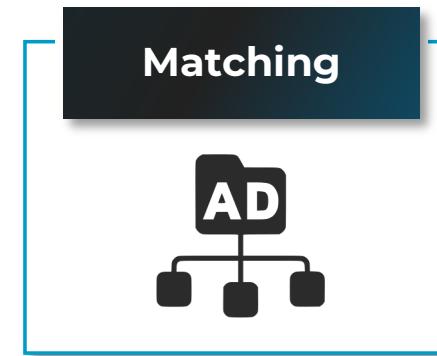
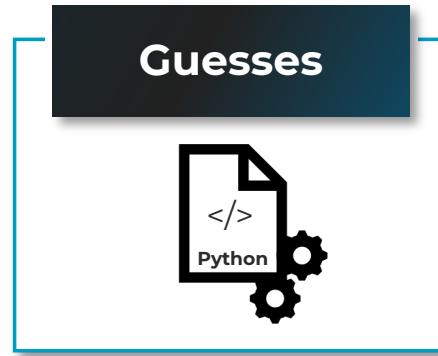
Survey



227,976 Usernames



Password Leaks & Compilations



450x Individual Leaks



12x Breach Compilations

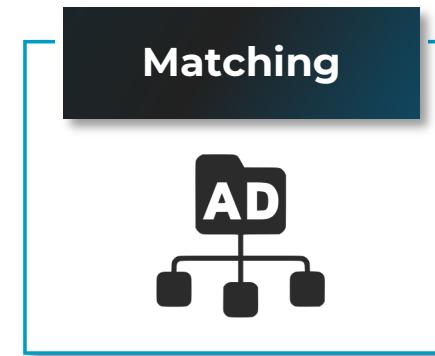


1.4B Breach Comp.
Collection #2
Big Database Comp.
Anti Public
Exploit.In
Onliner Spambot

Password Leaks

Name of Service	Reported Date of Breach	Date Breach Made Public	Categorization of Service [†]	Hash Function(s)	# of Credentials in Leak	# of Leaked Exact Email Matches	# of Leaked Similar Email Matches	# of Leaked Username Matches	Total # of Leaked Passwords	Total # of Password Guesses	# of Guesses Currently Valid	Total # of Correct Guesses
LinkedIn [38]	May 2012	May 2016	10	Unsalted SHA-1	164,611,595	4,901	190,980	9,309	195,110	91,784,381	533	2,433
Chegg [38]	Apr 2018	Aug 2019	5	Unsalted MD5	39,721,127	1,995	106,875	1,331	108,702	50,346,483	498	1,938
LiveJournal [38]	Jan 2017	May 2020	2	Plain Text	26,372,781	1,199	32,791	30,498	58,632	30,522,276	215	979
Dropbox [38]	Jul 2012	Aug 2016	19	SHA-1, bcrypt	68,648,009	698	40,565	3,177	41,013	21,041,006	287	903
MySpace [38]	Jul 2008	May 2016	14	SHA-1	359,420,698	1,934	456	111	1,976	1,042,004	108	767
Twitter * [62, 68]	Unknown	Jun 2016	14	Plain Text	32,800,000	347	43,967	55,077	74,970	38,988,904	124	396
Last.fm [38]	Mar 2012	Sep 2016	11	Unsalted MD5	37,217,682	626	144	166	626	351,506	17	217
Neopets [38]	May 2013	Jul 2016	8	Plain Text	26,892,897	138	33,140	26,040	57,665	26,786,340	45	129
Gmail * [68]	Unknown	Sep 2014	6	Plain Text	4,928,888	33	4,000	824	4,002	2,232,342	38	106
Zynga [38]	Sep 2019	Dec 2019	8	Salted SHA-1	172,869,660	33	3,998	821	3,998	2,230,421	38	106
Coupon Mom / Armor Games * [38]	Feb 2014	Nov 2017	13	Plain Text	11,010,525	135	18,441	1,196	18,533	9,441,013	33	99
Evony [38]	Jun 2016	Mar 2017	8	Plain Text	29,396,116	73	34,607	8,662	34,649	16,735,619	34	84
Zoosk * [38]	Jan 2011	Feb 2017	4	MD5	52,578,183	54	31,423	43,528	73,527	43,563,641	24	64
Fling [38]	Mar 2011	May 2016	4	Plain Text	40,767,652	65	40,540	29,987	67,915	29,447,501	23	62
Canva [38]	May 2019	Aug 2019	17	bcrypt	137,272,116	30	3,954	258	3,971	1,918,511	13	49
Stratfor [38]	Dec 2011	Dec 2013	12	Unsalted MD5	859,777	75	4,647	795	5,149	2,638,970	15	44
Brazzers [38]	Apr 2013	Sep 2016	0	Plain Text	790,724	24	2,117	3,022	4,457	2,269,866	11	40
Yahoo [38]	Jul 2012	Dec 2013	6	Plain Text	453,427	23	4,251	817	4,251	2,416,351	7	40
Wattpad [38]	Jun 2020	Jul 2020	11	bCrypt	268,765,495	8	3,126	2,011	4,655	2,158,286	16	39
Mate1 [38]	Feb 2016	Apr 2016	4	Plain Text	27,393,015	38	25,806	16,790	40,675	21,025,468	10	39
Forbes [38]	Feb 2014	Feb 2014	1	PHPass	1,057,819	16	843	1,573	2,137	1,093,803	9	28
Comcast [38]	Nov 2015	Feb 2016	19	Plain Text	616,882	3	3,072	3,073	3,073	1,748,416	10	26
VK [38]	Jan 2012	Jun 2016	14	Plain Text	93,338,602	34	32,743	4,385	35,072	17,931,318	8	25
Ashley Madison [38]	Jul 2015	Aug 2015	4	bCrypt	30,811,934	12	2,186	16,072	17,029	8,445,810	12	23
iMesh [38]	Sep 2013	Jul 2016	19	Salted MD5	49,467,477	37	11	4	37	17,849	2	19
XSplit [38]	Nov 2013	Aug 2015	8	Unsalted SHA-1	2,983,472	3	2,216	1,634	2,889	1,532,162	10	18
acne.org [38]	Nov 2014	Mar 2016	9	IPB	432,943	17	466	808	1,140	598,521	5	18
CheapAssGamer.com [38]	Jul 2015	Nov 2016	8	vBulletin	444,767	14	722	823	1,308	672,567	7	16
Dailymotion [38]	Oct 2016	Aug 2017	19	bCrypt	85,176,234	2	938	809	1,419	712,054	8	15
Tianya [38]	Dec 2011	Jun 2016	2	Plain Text	29,020,808	24	46,182	17,862	60,086	15,375,310	6	15
000webhost [38]	Mar 2015	Oct 2015	19	Plain Text	14,936,670	11	6,975	1,123	6,983	4,446,688	4	13
Android Forums [38]	Oct 2011	Dec 2015	2	vBulletin	745,355	3	427	562	767	395,897	2	10
Renren * [68]	Unknown	Dec 2011	14	Plain Text	4,768,600	40	13	10	40	20,995	0	10
Weibo * [68]	Unknown	Jan 2011	14	Plain Text	4,602,502	40	13	10	40	20,995	0	10
Patreon [38]	Oct 2015	Oct 2015	3	bCrypt	2,330,382	3	192	38	192	102,357	1	8
Rambler [38]	Mar 2014	Nov 2016	6	Plain Text	91,436,280	0	21,494	20,822	21,508	8,289,279	2	6
Lord of the Rings Online [38]	Aug 2013	Mar 2016	8	vBulletin	1,141,278	16	7	2	16	9,372	2	5
Taobao * [38]	Jan 2012	Oct 2016	13	Plain Text	21,149,008	0	9,936	173	9,936	5,011,503	2	5
Gamigo [38]	Mar 2012	Jan 2016	8	Unsalted MD5	8,243,604	3	4,284	440	4,284	2,792,297	1	5

Username Matching



username: **mgolla**

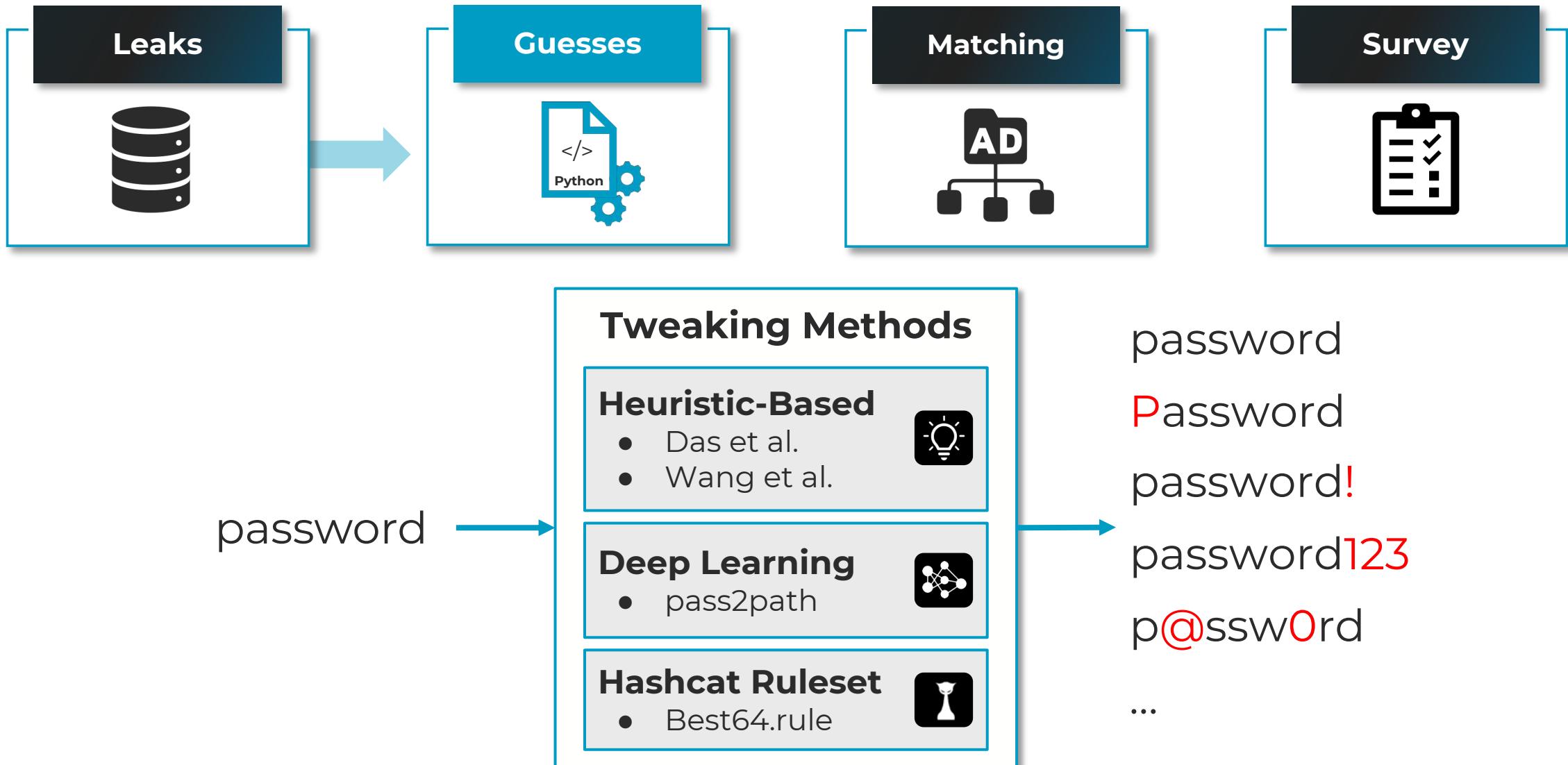
✓ **mgolla@uchicago.edu**

✓ **mgolla@cispa.de**

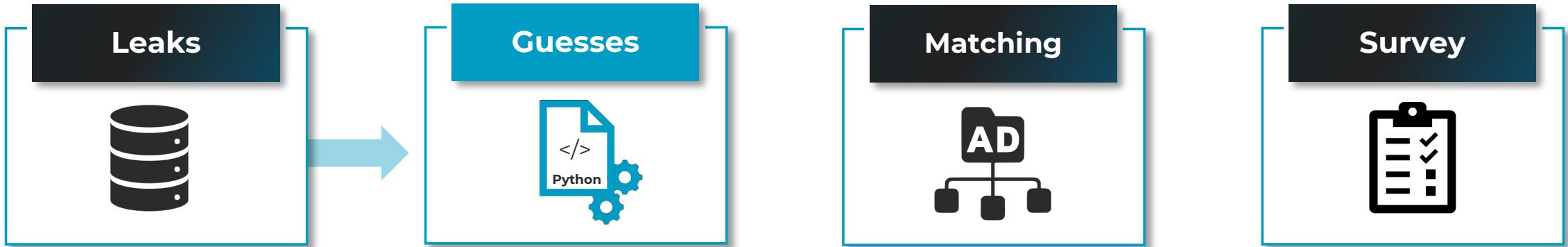
✓ **mgolla**

✗ **mgolla99@gmail.com**

Password Tweaking



Common Passwords

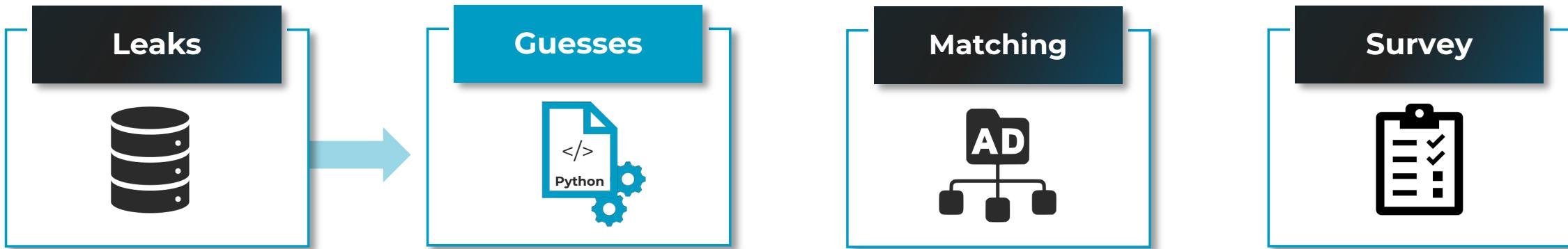


password1 → password1

LinkedIn1 → UChicago1

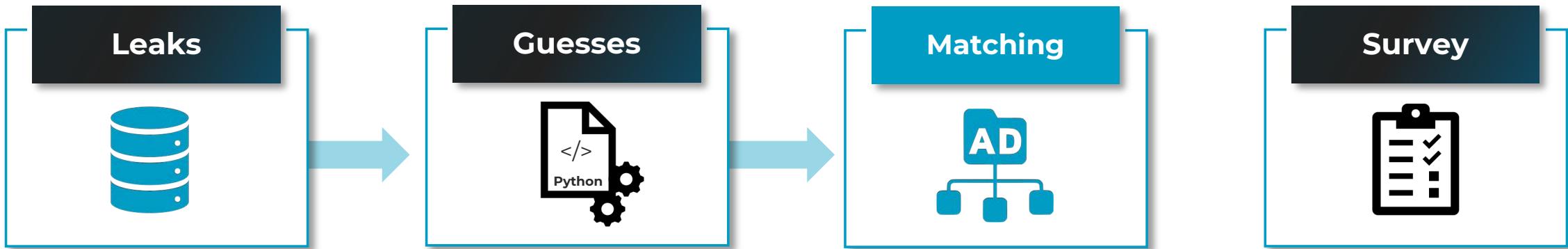
P@ssw0rd1234 → P@ssw0rd1234

UChicago's Password Policies



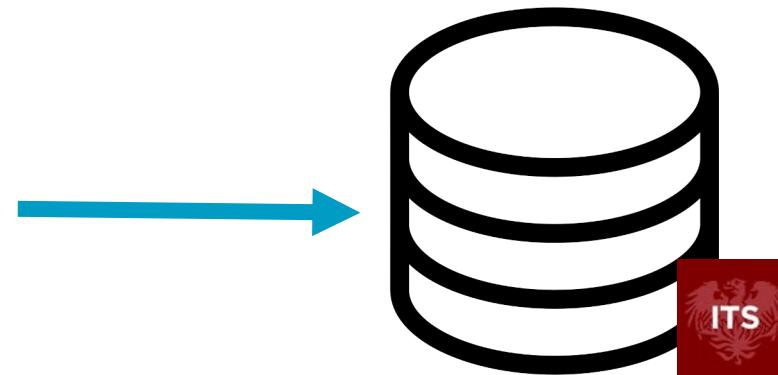
	Time Period	Length	Character Classes
Password	2015 - Present	12 - 19	3+
	2010 - 2015	8 - 16	3+
	Prior to 2010	8 - 16	2+
Passphrase	2016 - Present	18 - 32	1+
	2014 - 2016	18 - 50	1+

UChicago's IT Security Team



Username	Password	...
mwei	i<3cats2018!	...
mwei	i<3cats2019!	...
mgolla	Pf@nnkuchen99	...
...

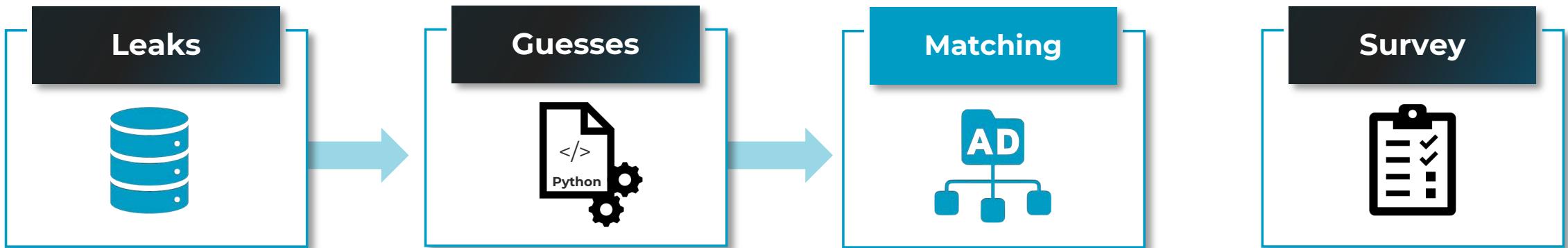
Our Guesses



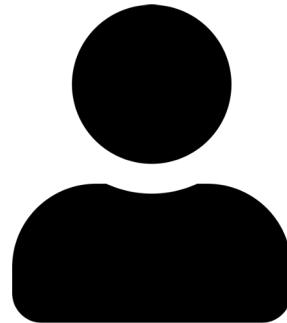
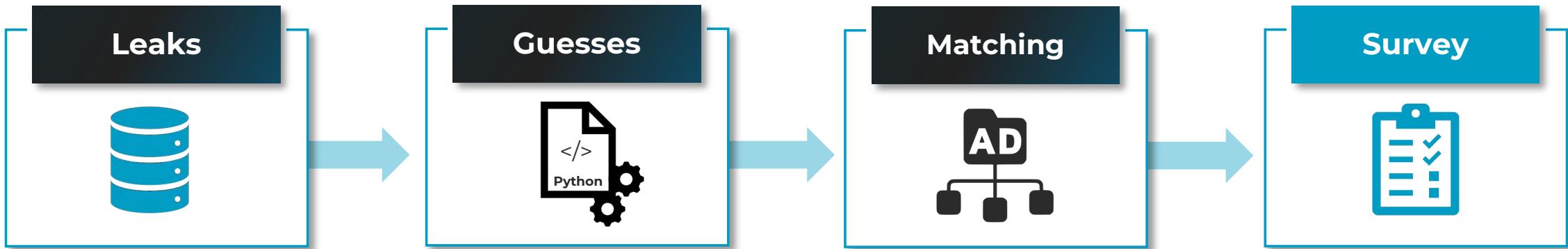
UChicago
Password History
Database

Accessed by
IT Services

Alert Affected Users



Users' Perceptions

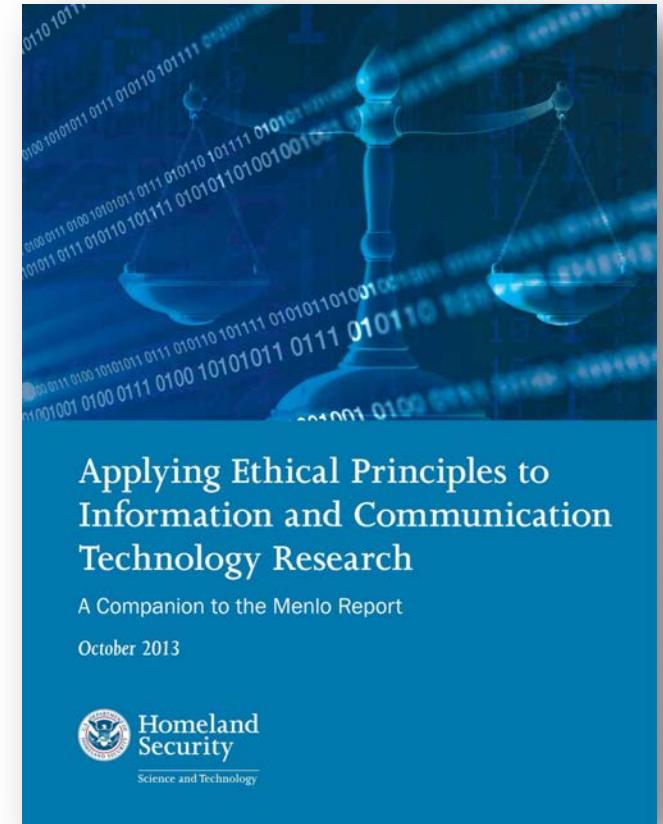


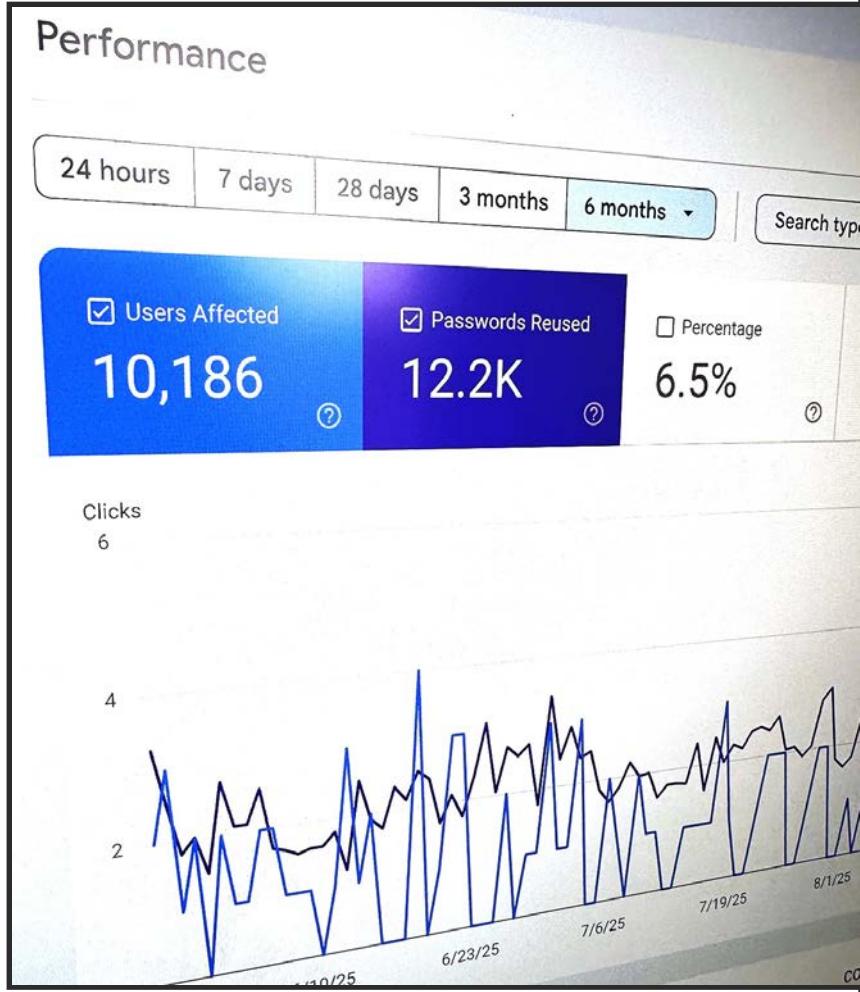
40 Participants

Surveys were customized to show participants the sources of data used to guess their password.

Ethics

- **IRB:** Approved by Institutional Review Board (IRB).
- **Stakeholders:** Study design informed by stakeholders.
- **Informed Consent:** Waiver; Affected users were notified.
- **Education:** We provided password security tips.
- **Access:** We did not have access to history database.
- **Re-Identification:** Limited meta-data (i.e., binned values).
- **Payment:** No payment for or redistribution of leaks.
- **Survey:** If data came from a sensitive leak (e.g., adult), we did not display the source in the survey.





Results

Where the data proudly disagrees with you.

So How Bad Is It?

12,247 correct guesses
based on password reuse (~ 5%)
([@gmail.com](mailto:mgolla@gmail.com)/[@hotmail.co.uk](mailto:mgolla@hotmail.co.uk)/[@web.de](mailto:mgolla@web.de))

Unfortunately, also
~ 32% of users with a [uchicago.edu](mailto:mgolla@uchicago.edu) email
in a data breach
(mgolla@uchicago.edu)

Give Me Numbers!

- **156,618** (out of 227,976) **usernames** were found in data leaks.
- **3,104,557 passwords** were found in leaks (of those 1,663,284 non-compliant).
- We generated **1,562,510,968 guesses** (all compliant).



14,161 total **correct guesses**.



12,247 from **password reuse** (affected 10,186 users).



1,979 from **common passwords** (affected 1,705 users).



35.5% of correct guesses were the user's **current password**.



These accounts required **forced resets**.



Attackers could have **compromised** them **at any time**.



Top Breaches Contributing Correct Guesses

Individual Leaks

 LinkedIn	2012	2,433
 Chegg	2018	1,938
 LiveJournal	2017	979
 Dropbox	2012	903
 myspace	2008	767
...

Breach Compilations

1.4B Breach Compilation	2017	7,715
Collection #2	2019	7,591
Big Database Combo List	2019	7,499
XSS.is 13B Account Leak	2019	6,960
Anti Public Combo List	2016	5,366
...

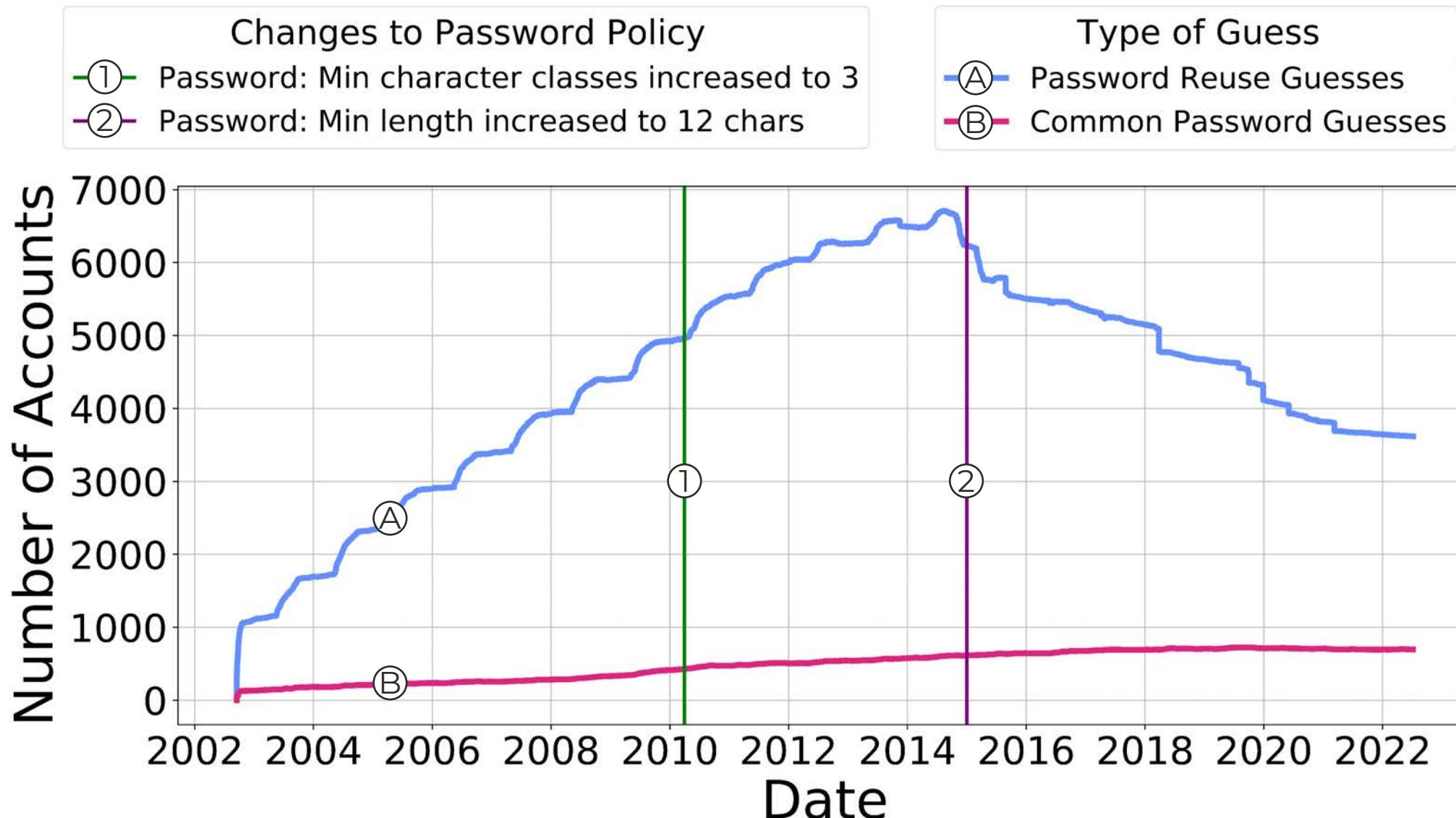


The “**classics**” still haunt users over **a decade later**.

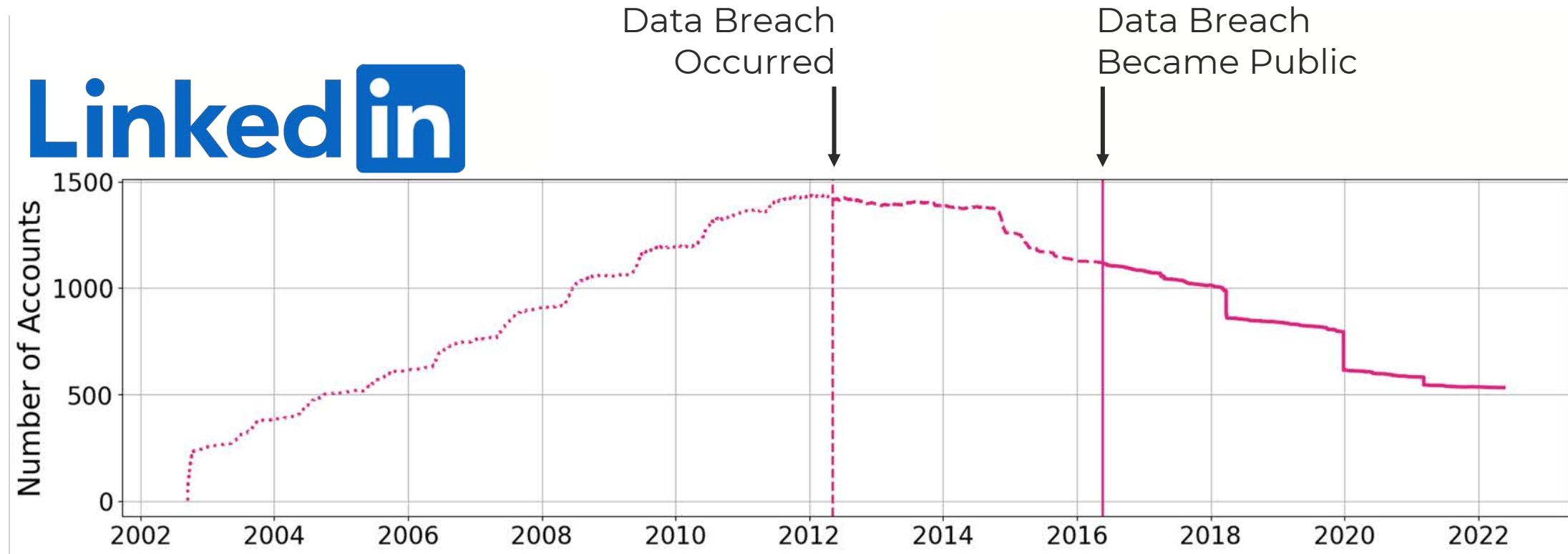


Breach **compilations** vastly **amplify** password reuse **attack surface**.

Password Reuse over Time

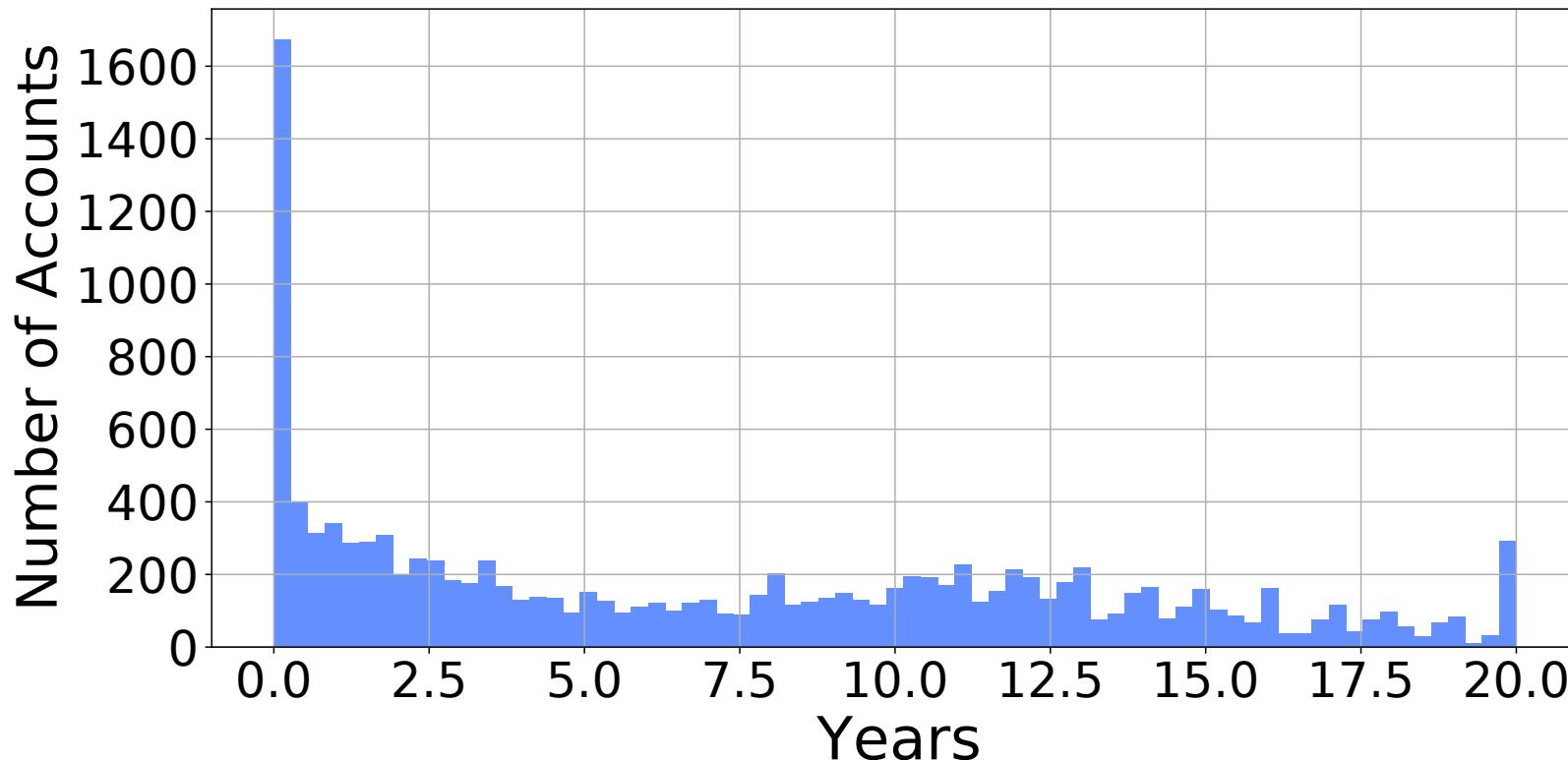


Reused Passwords Stay Valid for a Long Time

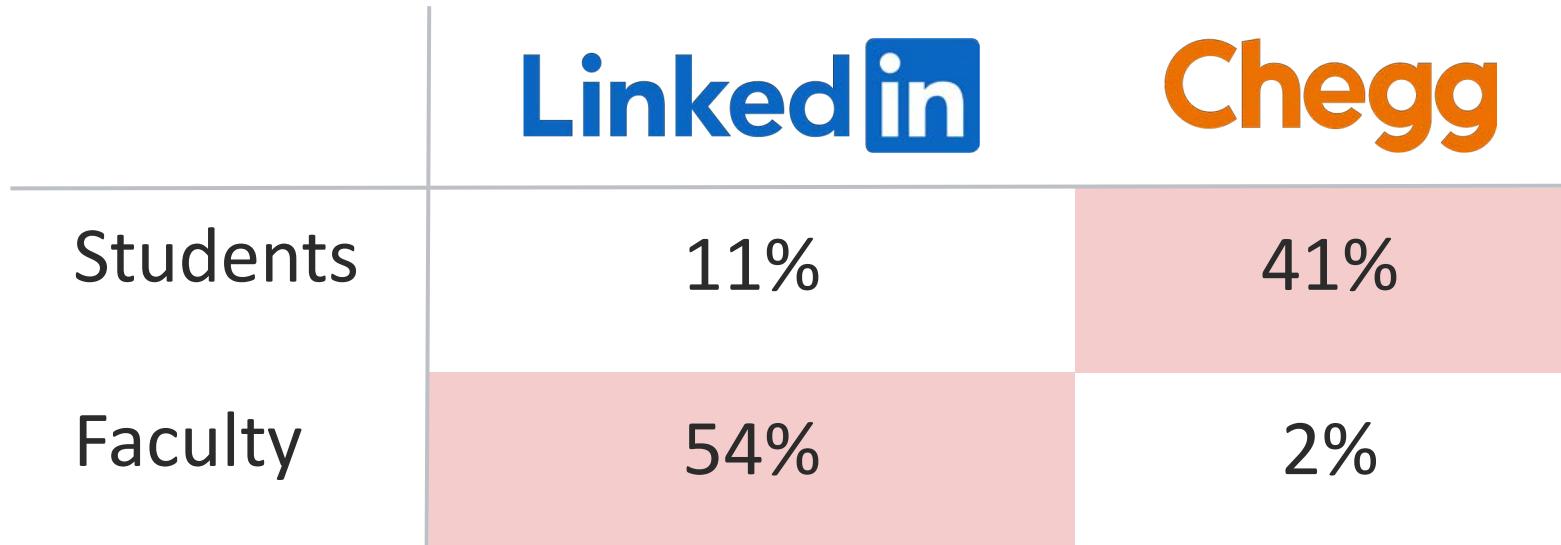


Password Lifetimes Are Shockingly Long

- Median lifetime: **6.2 years**.
- Max lifetime: **19.8 years**.
- Accounts **stay vulnerable for years** after a breach becomes public.



Data Breaches Impact on Specific Groups



Should We Try to Crack Hashes?

Plaintext

85%

Hashed

15%

Sunshine!

5F4DCC3B5AA765D61D8327DEB882CF99

correctbatteryhorsestaple

482C811DA5D5B4BC6D497FFA98491E38

i@mforg3tful!

62099D23A9D9910879D67449D9E084ED

ineedapassword

1C8F93D67A694EE1DE6363D20228DAC8

Exact or Tweaked Reuse?

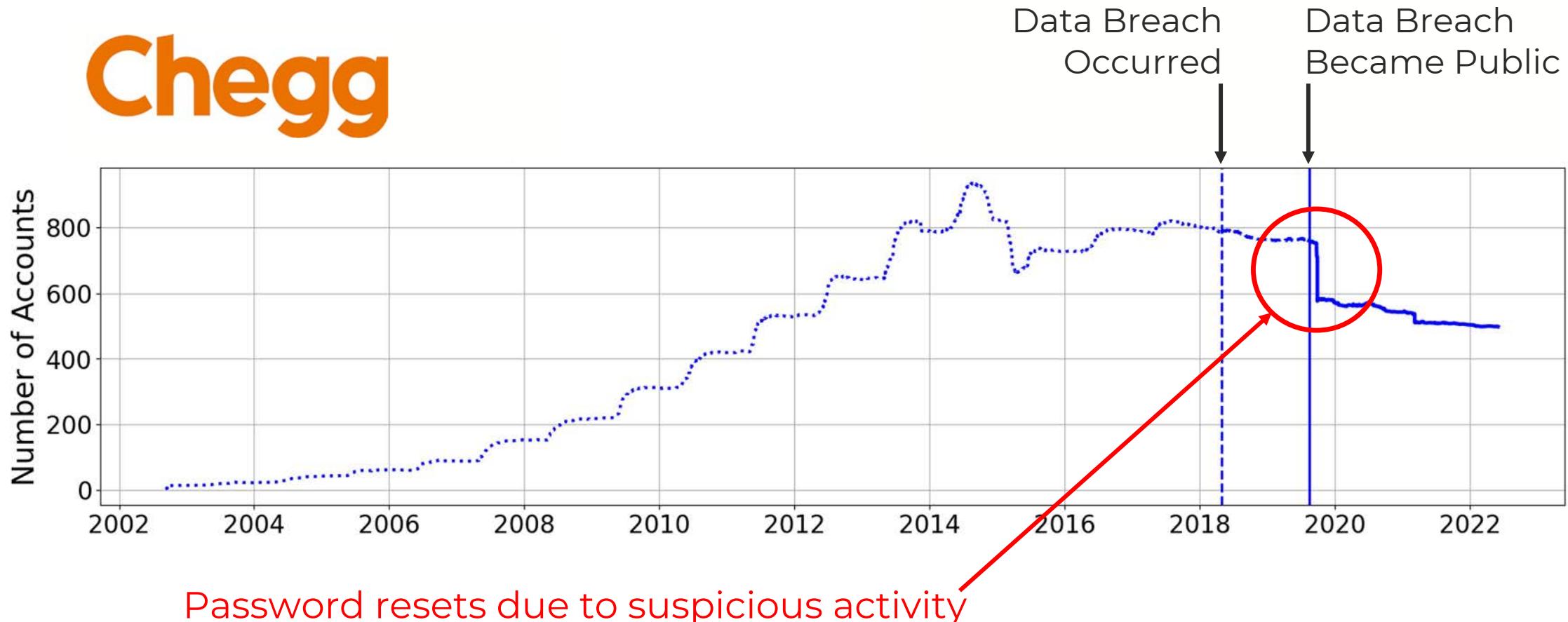
Verbatim
Reuse
55%

password → password123
p@ssw0rd
pa\$\$word

Tweaked
Passwords
45%

Reuse Is Being Exploited!

Chegg



Password resets due to suspicious activity

Evidence of Real-World Attacks

- All compromised accounts on **September 30th, 2019**, were found in the **Chegg** breach not long after it was added to HIBP on **August 16th, 2019**.
- 29x IT-flagged incidents involved 10+ accounts whose passwords we guessed.

Attack	Accounts	Source
March 2021	113	Breach Comp.
June 2020	115	LiveJournal
December 2019	206	LinkedIn
September 2019	134	Chegg
March 2018	291	Breach Comp.
...

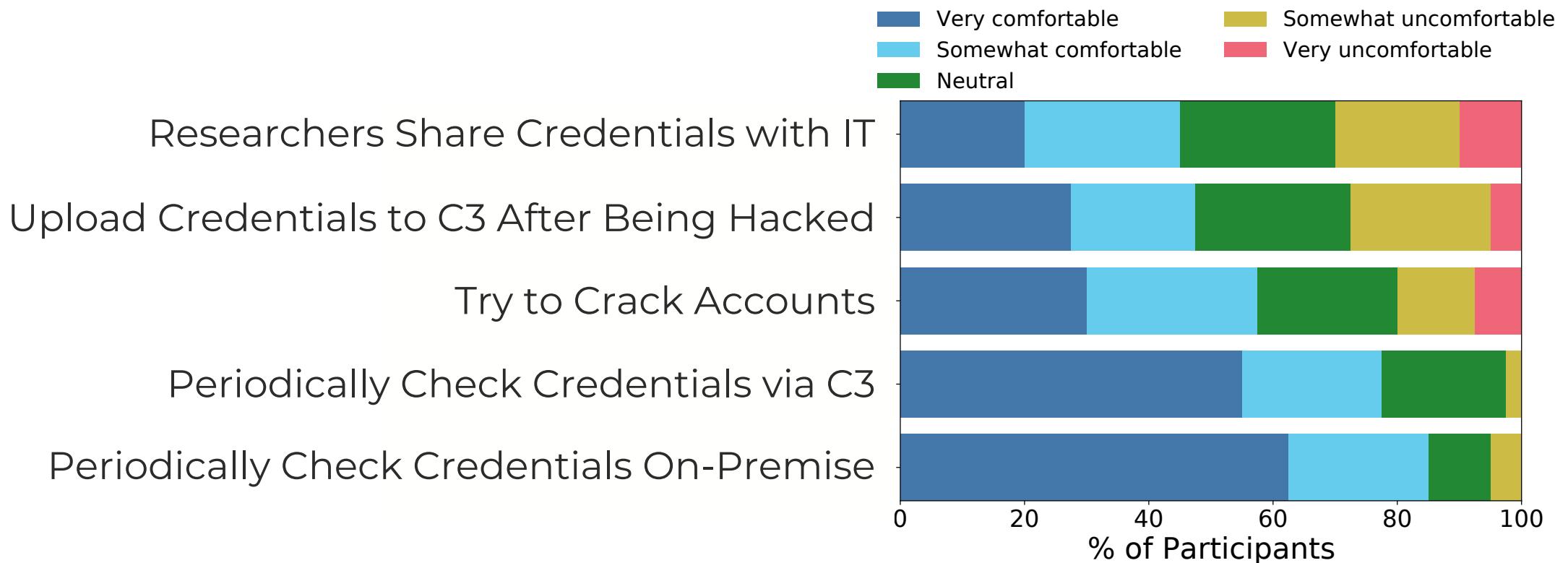


Cr3d0v3r by D4Vinci - v0.4
Know the dangers of credential stuffing attacks.
Loaded 14 university websites.

```
[+] Checking email in public leaks...
[+] HaveIBeenPwned website results: 1
[+] Name: Chegg | Date: 2019-08-16T23:35:45Z | What leaked: Usernames,Email addresses,Passwords
[!] [MIT] Login unsuccessful!
[!] [Stanford] Login unsuccessful!
[+] [UChicago] Login successful!
```

Survey of Affected Users (n=40)

- 68% of the survey participants had their *current* password guessed and reset.
- Many **unaware** they **had accounts on breached services**.
- Many **unaware** of the **risk caused by password reuse**.
- **Almost nobody knew** that their **password** was **compromised years earlier**.

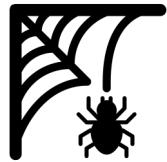




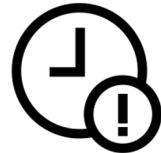
Discussion

Where speculation becomes 'future work.'

Now What?



Implement processes to **expire unused accounts**.



Promptly check high-risk (i.e., **organization-related breaches**) when they become public.

HIBP



Also check for reuse of **hashed and tweaked passwords** in less common data breaches.



Check for **similar email** and **username matches**, not only exact email matches.

Takeaway

Reuse Vulnerability

Reuse is a **greater threat** than **common** passwords.

UChicago began **requiring** current faculty, staff, and students to use **2FA**.

Long-Lasting

Accounts **vulnerable for long periods** (years!).

Reactive checks failed as passwords predated breaches.

Proactive Approach

Checking of credentials **at creation and periodically afterward**.

Expiration of unused accounts.



THE UNIVERSITY OF
CHICAGO



Alexandra Nisenoff, Maximilian Golla, Miranda Wei, Juliette Hainline, Hayley Szymanek, Annika Braun, Annika Hildebrandt, Blair Christensen, David Langenberg, and Blase Ur.