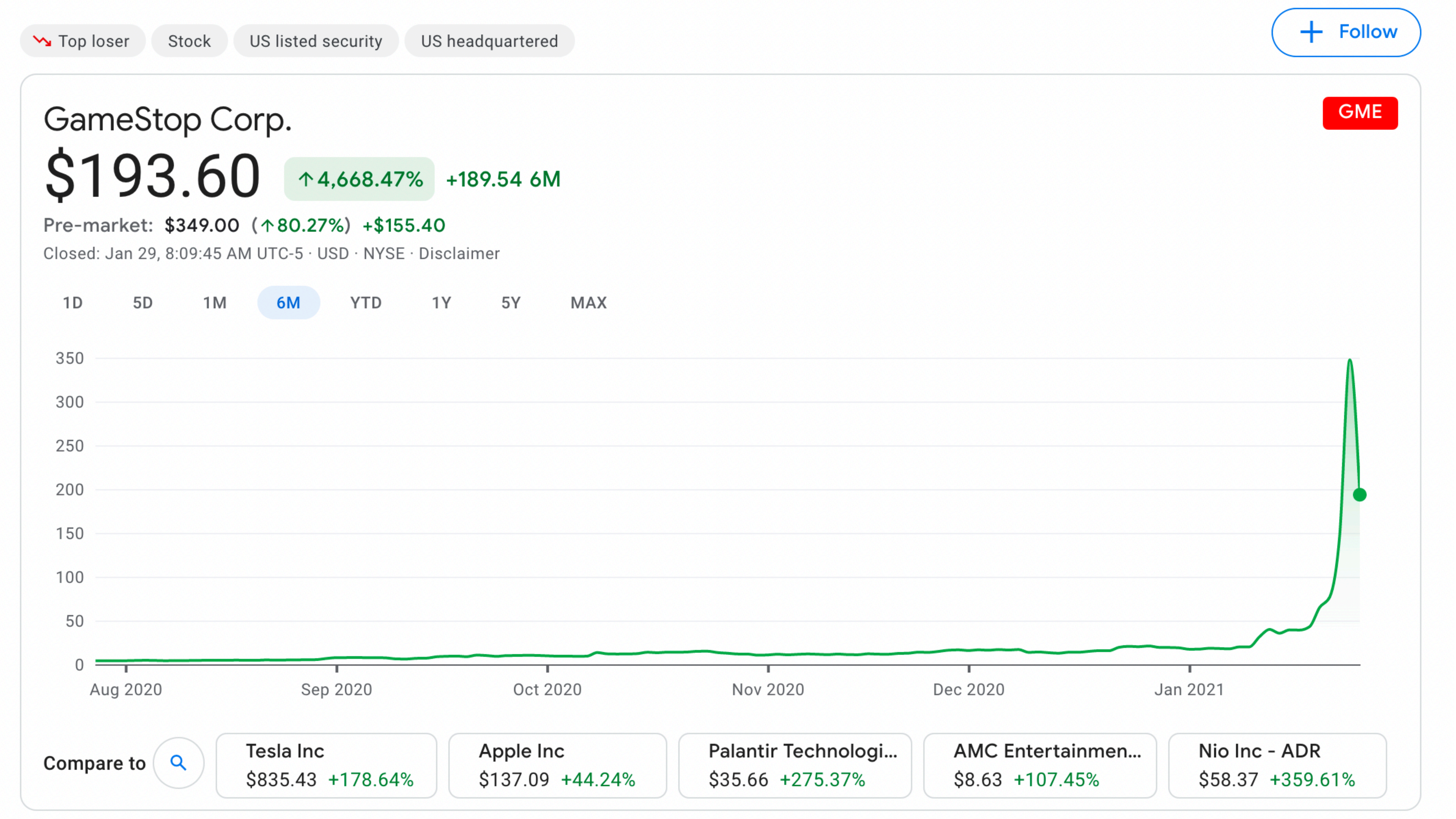
2550 Intro to cybersecurity

L4

abhi shelat

GME



Top loser · Stock · US listed security · US headquartered

GameStop Corp.

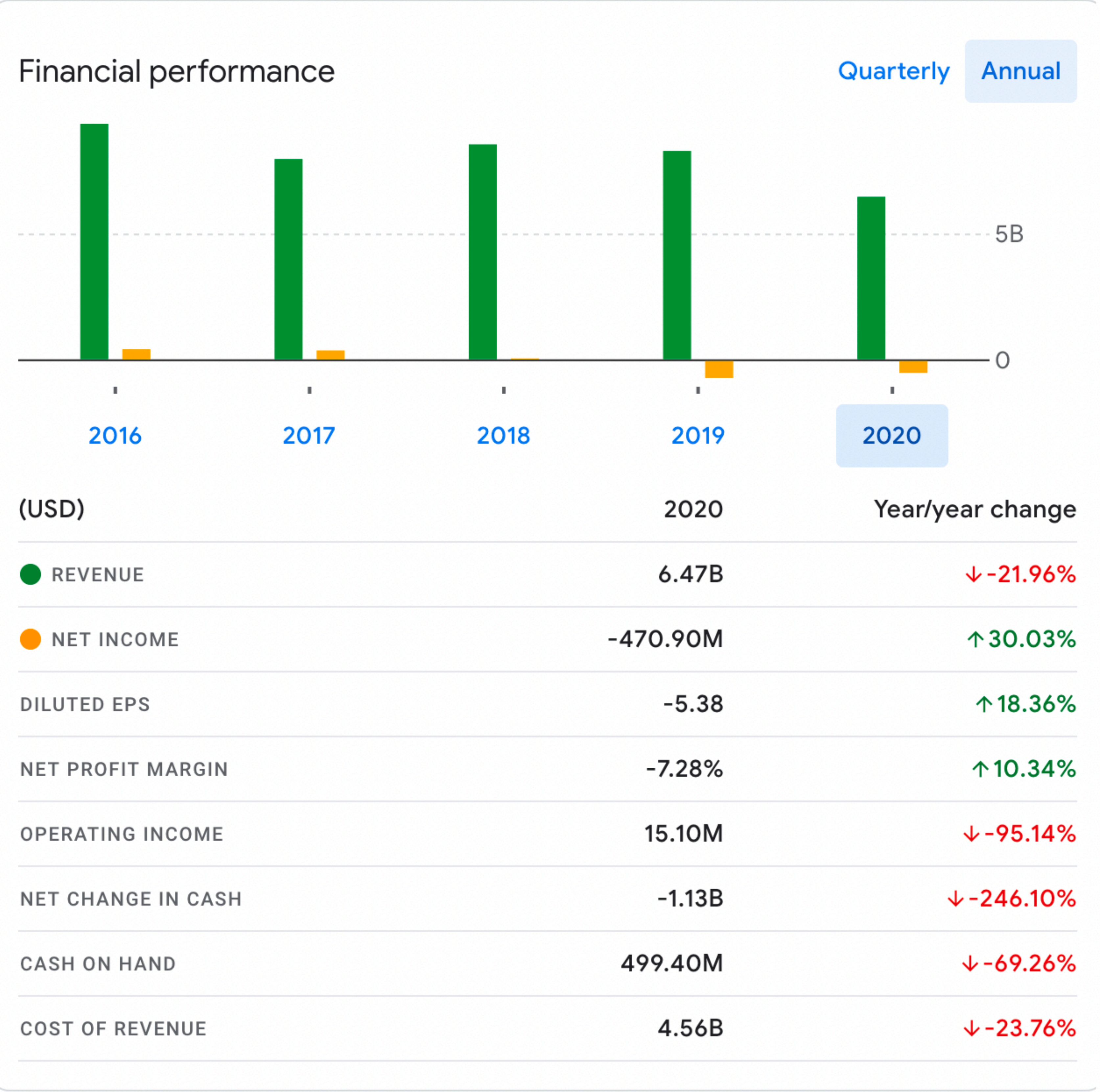
$193.60 ↑4,668.47% +189.54 6M

Pre-market: $349.00 (↑80.27%) +$155.40

Closed: Jan 29, 8:09:45 AM UTC-5 · USD · NYSE · Disclaimer

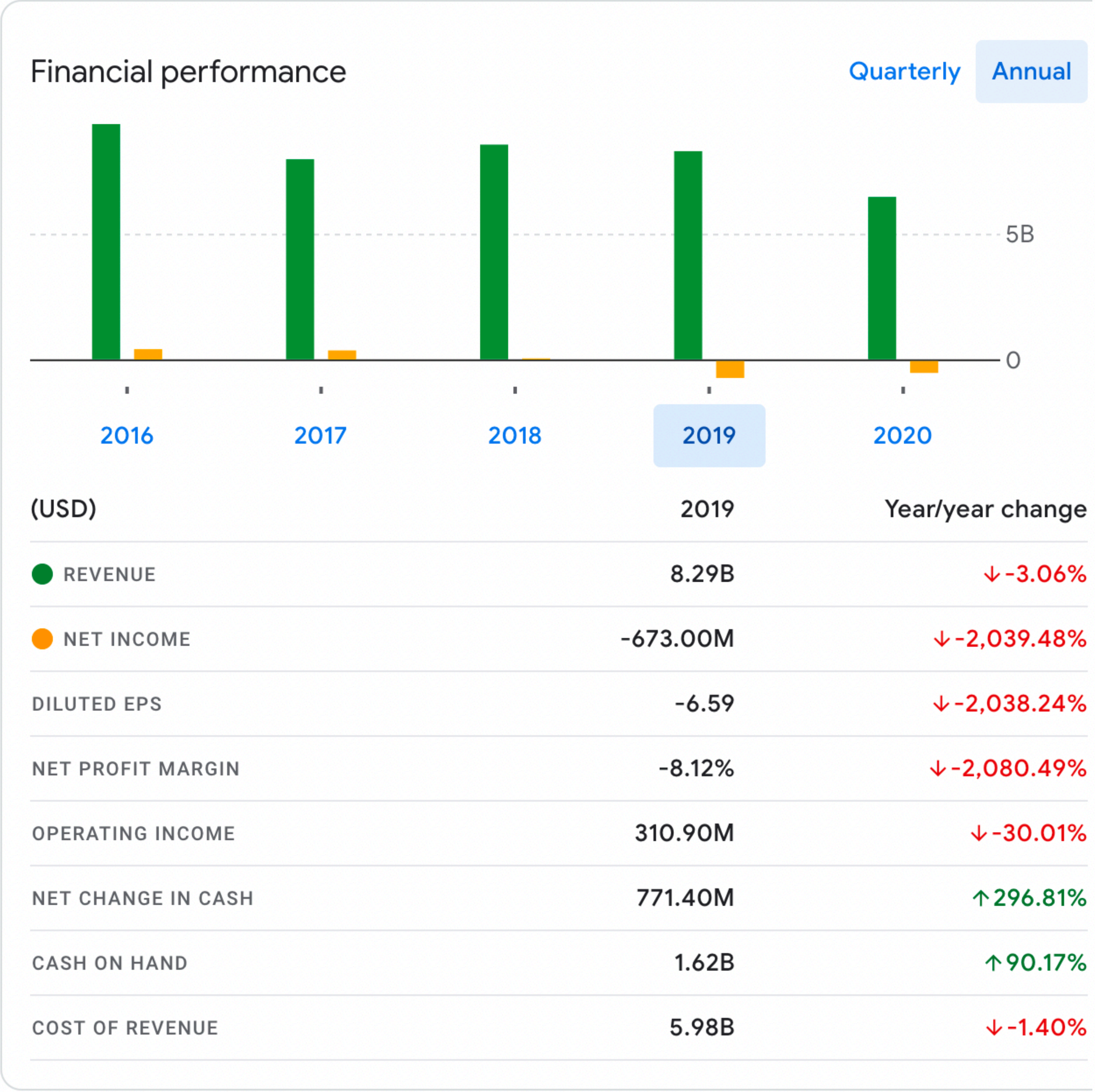
Compare to

Tesla Inc	$835.43 +178.64%
Apple Inc	$137.09 +44.24%
Palantir Technologi...	$35.66 +275.37%
AMC Entertainmen...	$8.63 +107.45%
Nio Inc - ADR	$58.37 +359.61%



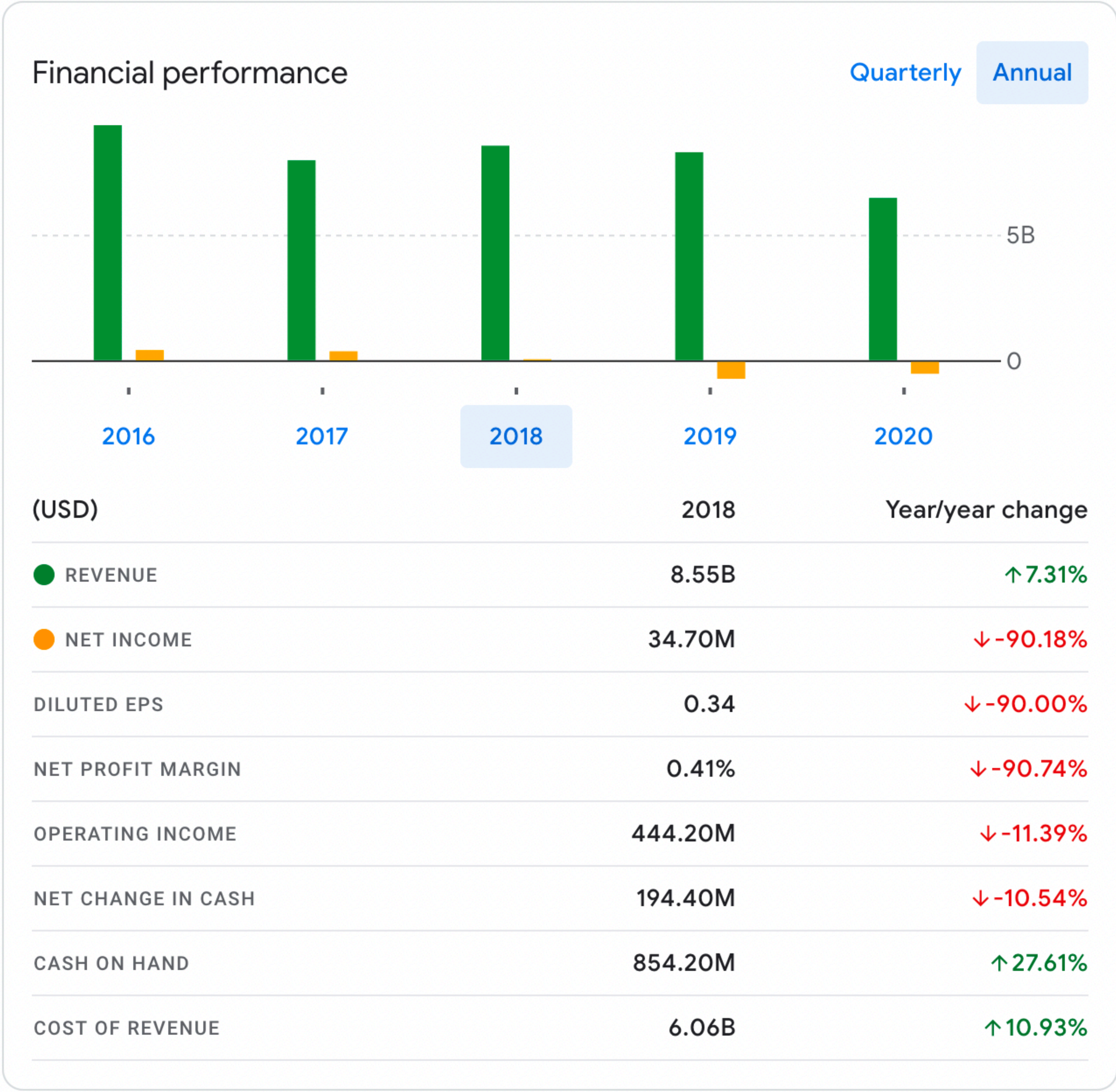
Financial performance

(USD)	2020	Year/year change
● REVENUE	6.47B	↓-21.96%
● NET INCOME	-470.90M	↑30.03%
DILUTED EPS	-5.38	↑18.36%
NET PROFIT MARGIN	-7.28%	↑10.34%
OPERATING INCOME	15.10M	↓-95.14%
NET CHANGE IN CASH	-1.13B	↓-246.10%
CASH ON HAND	499.40M	↓-69.26%
COST OF REVENUE	4.56B	↓-23.76%



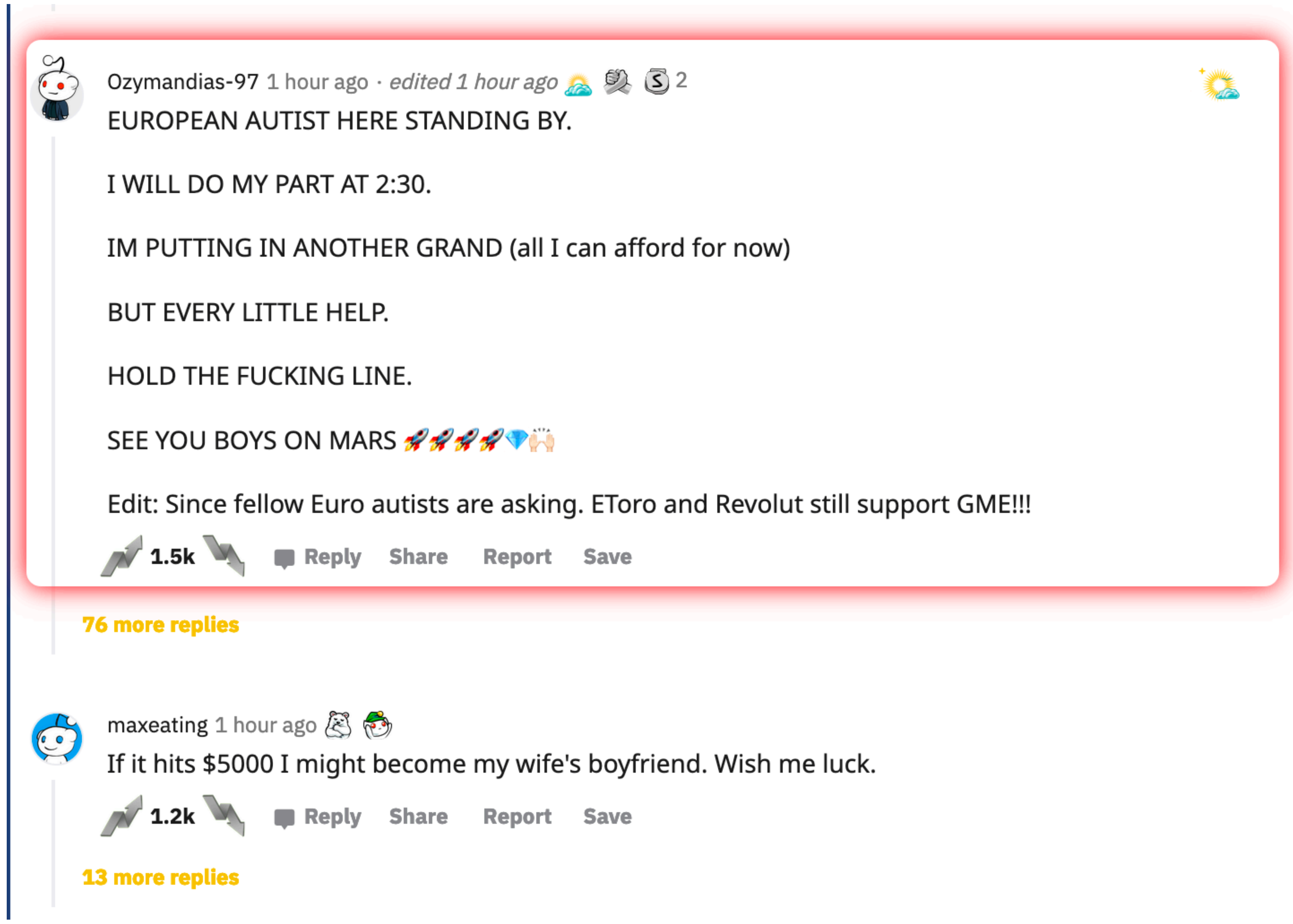
Financial performance

(USD)	2019	Year/year change
● REVENUE	8.29B	↓-3.06%
● NET INCOME	-673.00M	↓-2,039.48%
DILUTED EPS	-6.59	↓-2,038.24%
NET PROFIT MARGIN	-8.12%	↓-2,080.49%
OPERATING INCOME	310.90M	↓-30.01%
NET CHANGE IN CASH	771.40M	↑296.81%
CASH ON HAND	1.62B	↑90.17%
COST OF REVENUE	5.98B	↓-1.40%



Financial performance

(USD)	2018	Year/year change
● REVENUE	8.55B	↑7.31%
● NET INCOME	34.70M	↓-90.18%
DILUTED EPS	0.34	↓-90.00%
NET PROFIT MARGIN	0.41%	↓-90.74%
OPERATING INCOME	444.20M	↓-11.39%
NET CHANGE IN CASH	194.40M	↓-10.54%
CASH ON HAND	854.20M	↑27.61%
COST OF REVENUE	6.06B	↑10.93%



Ozymandias-97 1 hour ago · *edited 1 hour ago* 2

EUROPEAN AUTIST HERE STANDING BY.

I WILL DO MY PART AT 2:30.

IM PUTTING IN ANOTHER GRAND (all I can afford for now)

BUT EVERY LITTLE HELP.

HOLD THE FUCKING LINE.

SEE YOU BOYS ON MARS 🚀🚀🚀🚀💎🙌

Edit: Since fellow Euro autists are asking. EToro and Revolut still support GME!!!

1.5k Reply Share Report Save

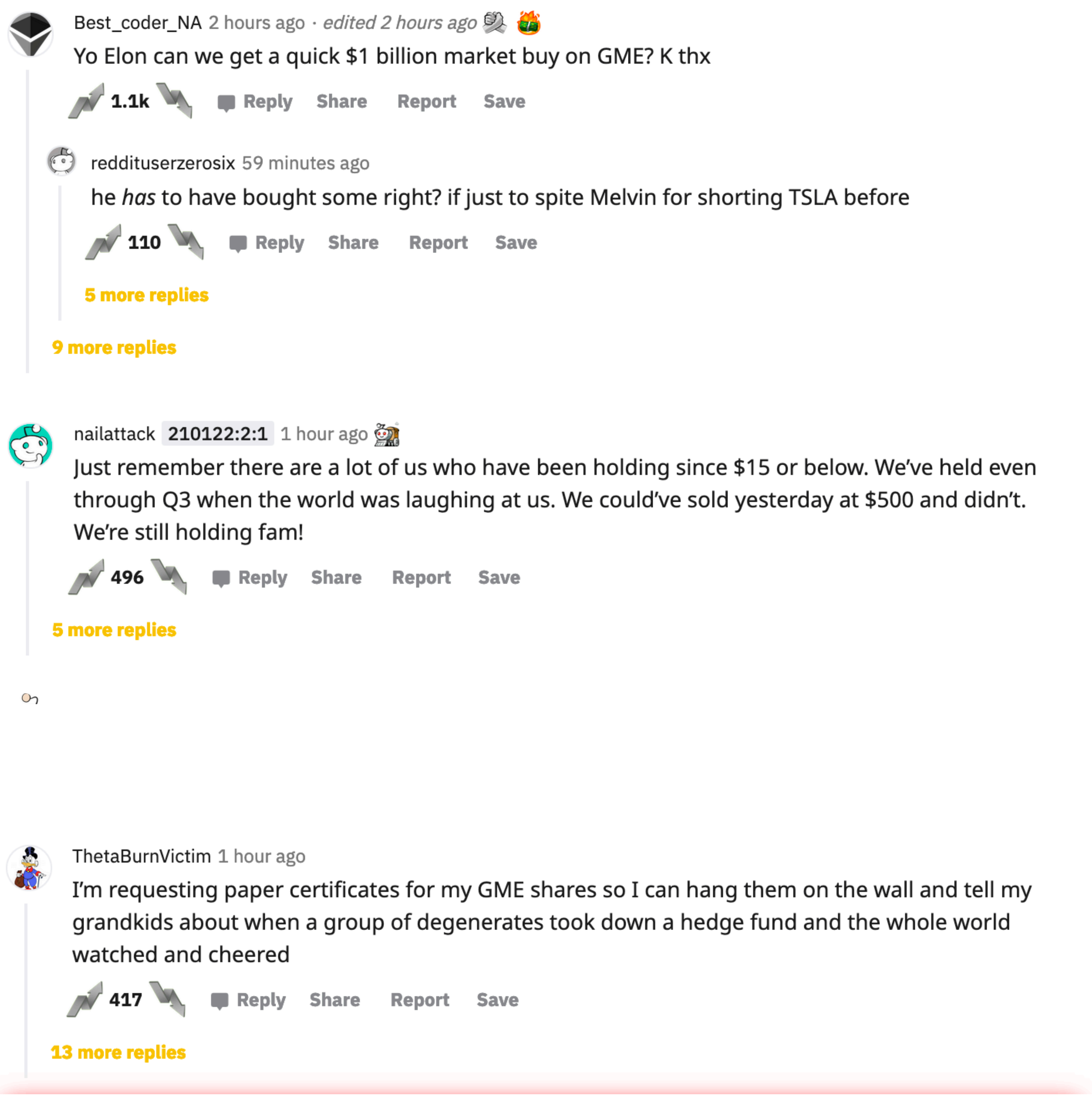
76 more replies

maxeating 1 hour ago

If it hits $5000 I might become my wife's boyfriend. Wish me luck.

1.2k Reply Share Report Save

13 more replies



Best_coder_NA 2 hours ago · *edited 2 hours ago*

Yo Elon can we get a quick $1 billion market buy on GME? K thx

1.1k Reply Share Report Save

reddituserzerosix 59 minutes ago

he *has* to have bought some right? if just to spite Melvin for shorting TSLA before

110 Reply Share Report Save

5 more replies

9 more replies

nailattack 210122:2:1 1 hour ago

Just remember there are a lot of us who have been holding since $15 or below. We've held even through Q3 when the world was laughing at us. We could've sold yesterday at $500 and didn't. We're still holding fam!

496 Reply Share Report Save

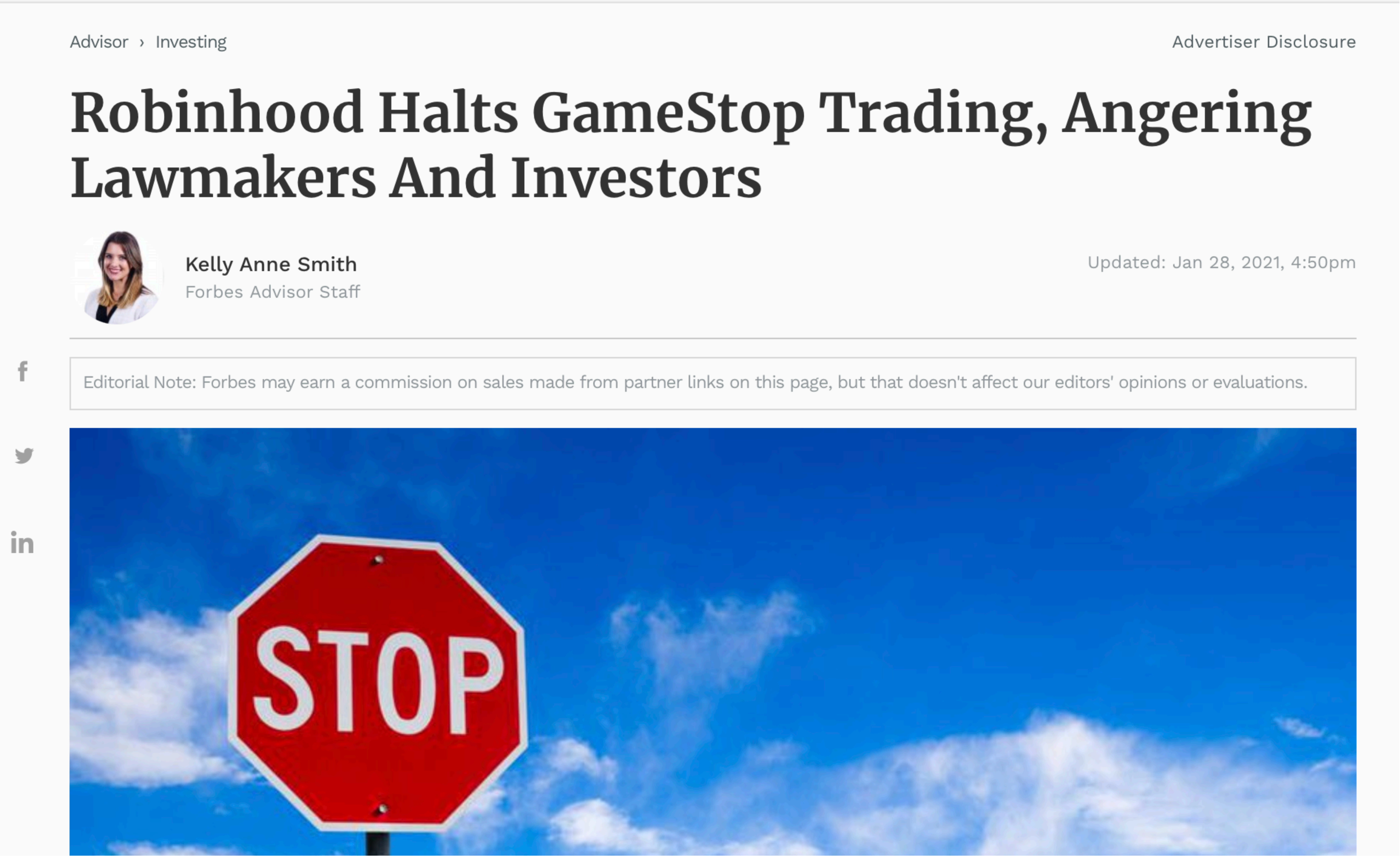
5 more replies

Theta BurnVictim 1 hour ago

I'm requesting paper certificates for my GME shares so I can hang them on the wall and tell my grandkids about when a group of degenerates took down a hedge fund and the whole world watched and cheered

417 Reply Share Report Save

13 more replies



Advisor › Investing

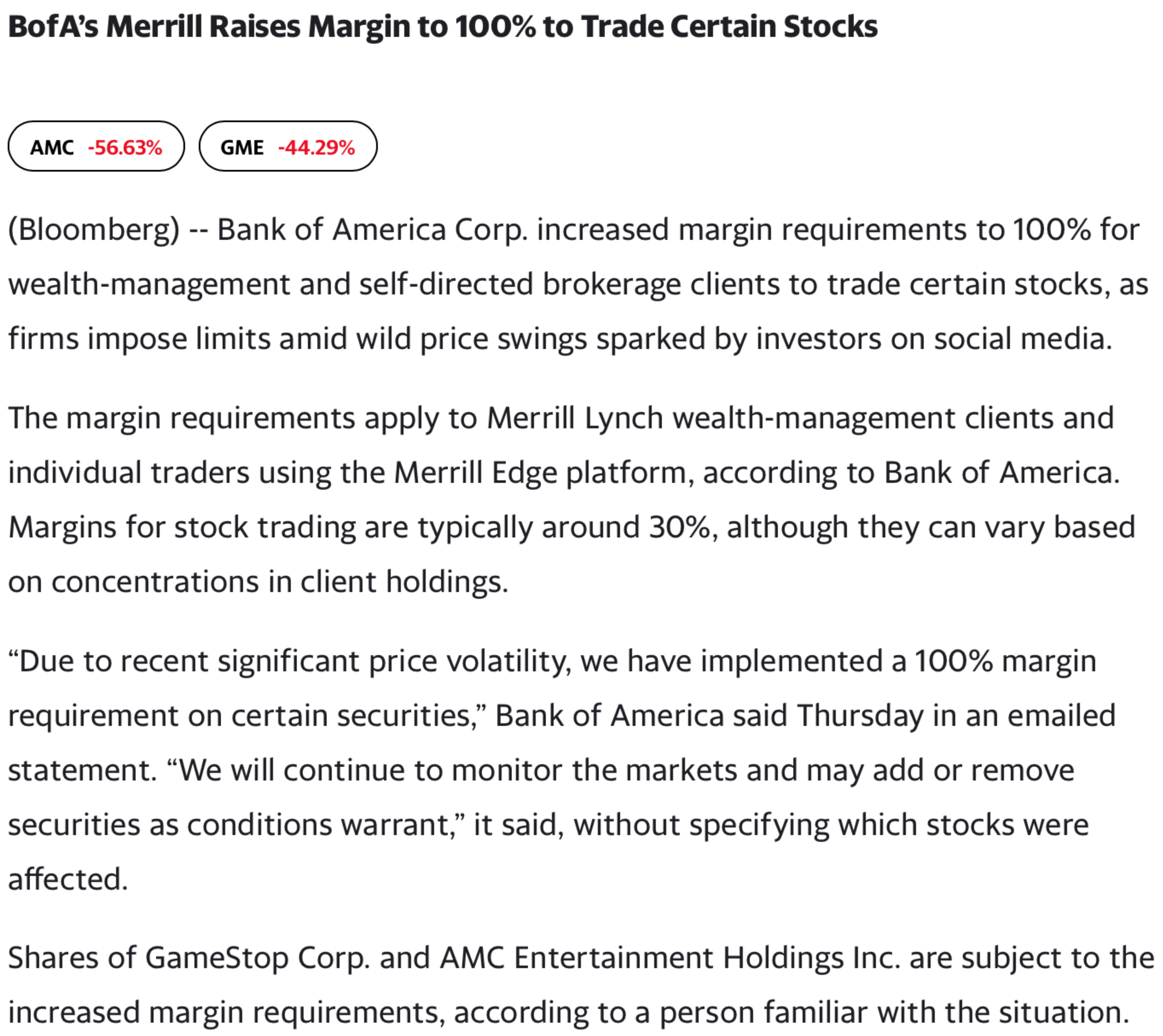
Advertiser Disclosure

Robinhood Halts GameStop Trading, Angering Lawmakers And Investors

Kelly Anne Smith
Forbes Advisor Staff

Updated: Jan 28, 2021, 4:50pm

Editorial Note: Forbes may earn a commission on sales made from partner links on this page, but that doesn't affect our editors' opinions or evaluations.



BofA's Merrill Raises Margin to 100% to Trade Certain Stocks

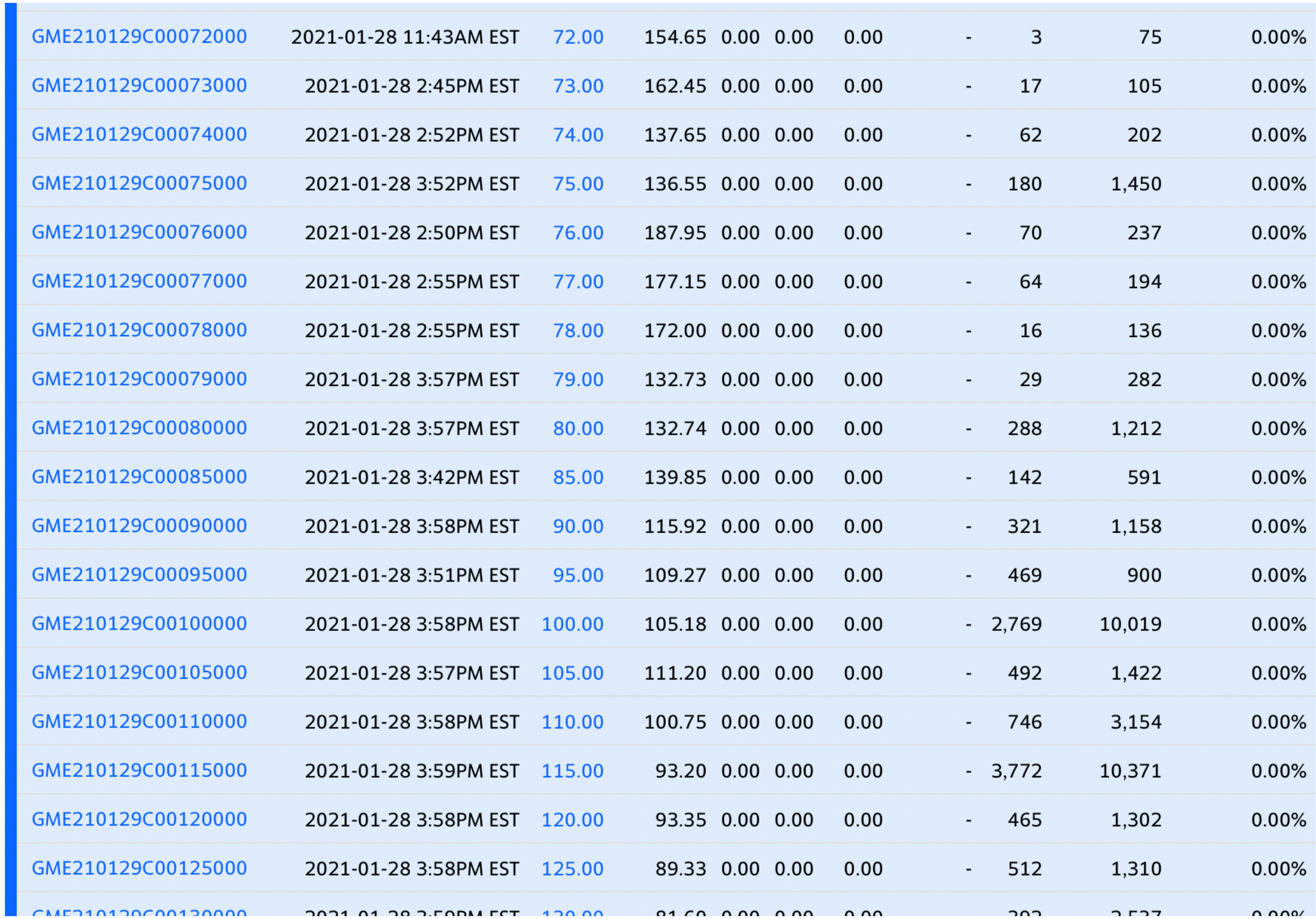
AMC -56.63% GME -44.29%

(Bloomberg) -- Bank of America Corp. increased margin requirements to 100% for wealth-management and self-directed brokerage clients to trade certain stocks, as firms impose limits amid wild price swings sparked by investors on social media.

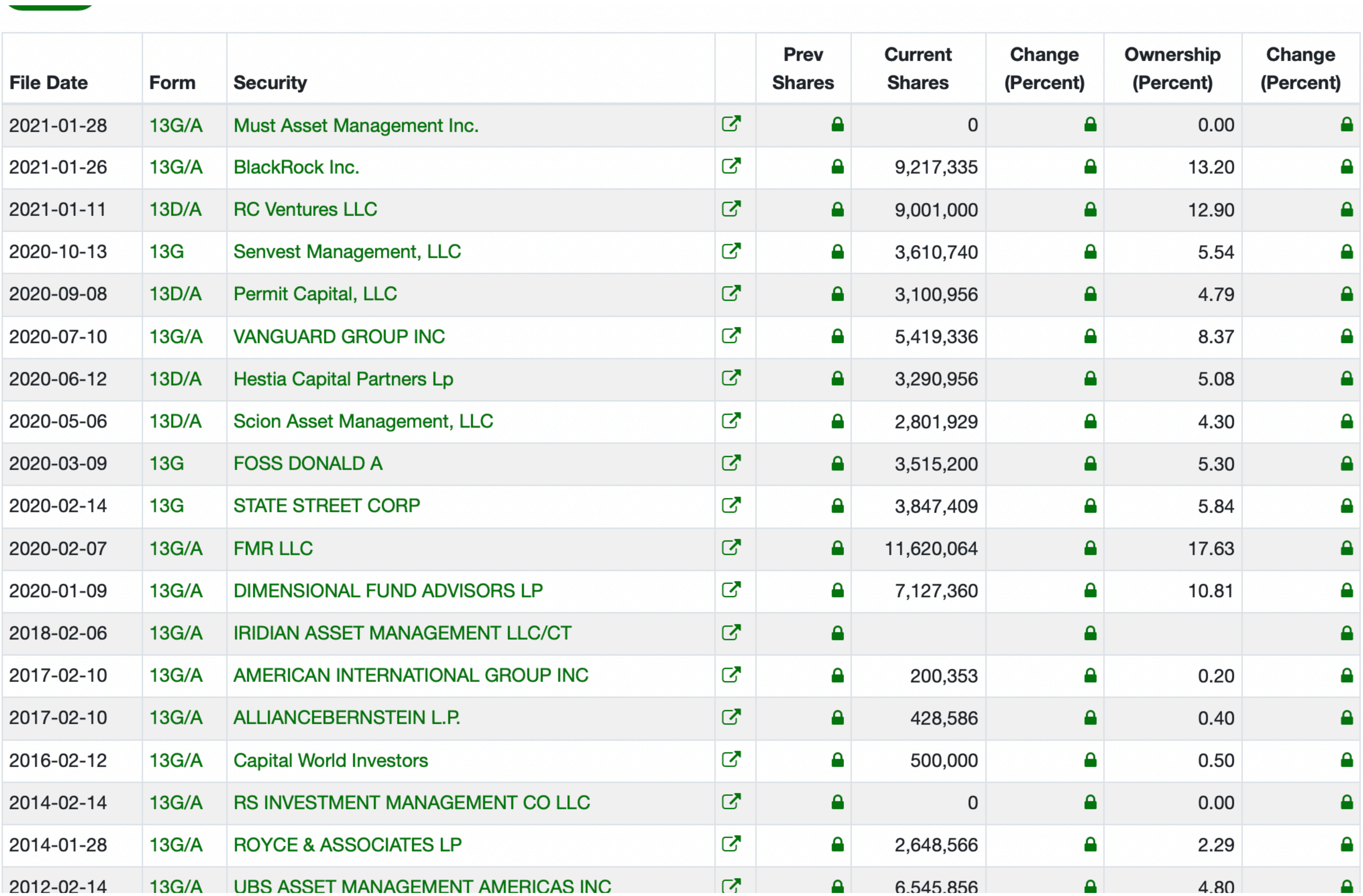
The margin requirements apply to Merrill Lynch wealth-management clients and individual traders using the Merrill Edge platform, according to Bank of America. Margins for stock trading are typically around 30%, although they can vary based on concentrations in client holdings.

"Due to recent significant price volatility, we have implemented a 100% margin requirement on certain securities," Bank of America said Thursday in an emailed statement. "We will continue to monitor the markets and may add or remove securities as conditions warrant," it said, without specifying which stocks were affected.

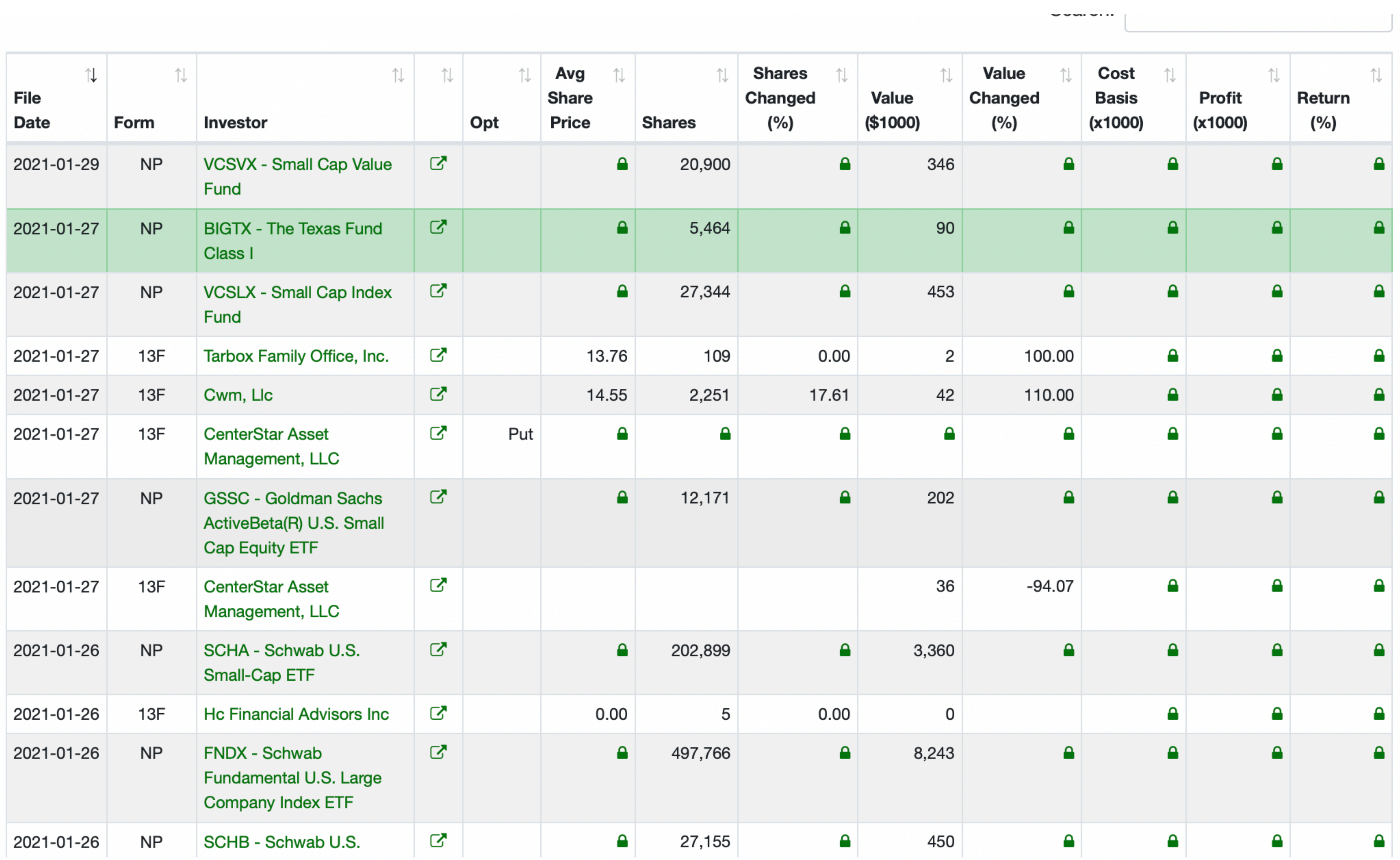
Shares of GameStop Corp. and AMC Entertainment Holdings Inc. are subject to the increased margin requirements, according to a person familiar with the situation.



GME210129C00072000	2021-01-28 11:43AM EST	72.00	154.65	0.00	0.00	0.00	-	3	75	0.00%
GME210129C00073000	2021-01-28 2:45PM EST	73.00	162.45	0.00	0.00	0.00	-	17	105	0.00%
GME210129C00074000	2021-01-28 2:52PM EST	74.00	137.65	0.00	0.00	0.00	-	62	202	0.00%
GME210129C00075000	2021-01-28 3:52PM EST	75.00	136.55	0.00	0.00	0.00	-	180	1,450	0.00%
GME210129C00076000	2021-01-28 2:50PM EST	76.00	187.95	0.00	0.00	0.00	-	70	237	0.00%
GME210129C00077000	2021-01-28 2:55PM EST	77.00	177.15	0.00	0.00	0.00	-	64	194	0.00%
GME210129C00078000	2021-01-28 2:55PM EST	78.00	172.00	0.00	0.00	0.00	-	16	136	0.00%
GME210129C00079000	2021-01-28 3:57PM EST	79.00	132.73	0.00	0.00	0.00	-	29	282	0.00%
GME210129C00080000	2021-01-28 3:57PM EST	80.00	132.74	0.00	0.00	0.00	-	288	1,212	0.00%
GME210129C00085000	2021-01-28 3:42PM EST	85.00	139.85	0.00	0.00	0.00	-	142	591	0.00%
GME210129C00090000	2021-01-28 3:58PM EST	90.00	115.92	0.00	0.00	0.00	-	321	1,158	0.00%
GME210129C00095000	2021-01-28 3:51PM EST	95.00	109.27	0.00	0.00	0.00	-	469	900	0.00%
GME210129C00100000	2021-01-28 3:58PM EST	100.00	105.18	0.00	0.00	0.00	-	2,769	10,019	0.00%
GME210129C00105000	2021-01-28 3:57PM EST	105.00	111.20	0.00	0.00	0.00	-	492	1,422	0.00%
GME210129C00110000	2021-01-28 3:58PM EST	110.00	100.75	0.00	0.00	0.00	-	746	3,154	0.00%
GME210129C00115000	2021-01-28 3:59PM EST	115.00	93.20	0.00	0.00	0.00	-	3,772	10,371	0.00%
GME210129C00120000	2021-01-28 3:58PM EST	120.00	93.35	0.00	0.00	0.00	-	465	1,302	0.00%
GME210129C00125000	2021-01-28 3:58PM EST	125.00	89.33	0.00	0.00	0.00	-	512	1,310	0.00%
GME210129C00130000	2021-01-28 3:59PM EST	130.00	81.60	0.00	0.00	0.00	-	393	2,537	0.00%



File Date	Form	Security		Prev Shares	Current Shares	Change (Percent)	Ownership (Percent)	Change (Percent)
2021-01-28	13G/A	Must Asset Management Inc.	↗	🔒	0	🔒	0.00	🔒
2021-01-26	13G/A	BlackRock Inc.	↗	🔒	9,217,335	🔒	13.20	🔒
2021-01-11	13D/A	RC Ventures LLC	↗	🔒	9,001,000	🔒	12.90	🔒
2020-10-13	13G	Senvest Management, LLC	↗	🔒	3,610,740	🔒	5.54	🔒
2020-09-08	13D/A	Permit Capital, LLC	↗	🔒	3,100,956	🔒	4.79	🔒
2020-07-10	13G/A	VANGUARD GROUP INC	↗	🔒	5,419,336	🔒	8.37	🔒
2020-06-12	13D/A	Hestia Capital Partners Lp	↗	🔒	3,290,956	🔒	5.08	🔒
2020-05-06	13D/A	Scion Asset Management, LLC	↗	🔒	2,801,929	🔒	4.30	🔒
2020-03-09	13G	FOSS DONALD A	↗	🔒	3,515,200	🔒	5.30	🔒
2020-02-14	13G	STATE STREET CORP	↗	🔒	3,847,409	🔒	5.84	🔒
2020-02-07	13G/A	FMR LLC	↗	🔒	11,620,064	🔒	17.63	🔒
2020-01-09	13G/A	DIMENSIONAL FUND ADVISORS LP	↗	🔒	7,127,360	🔒	10.81	🔒
2018-02-06	13G/A	IRIDIAN ASSET MANAGEMENT LLC/CT	↗	🔒		🔒		🔒
2017-02-10	13G/A	AMERICAN INTERNATIONAL GROUP INC	↗	🔒	200,353	🔒	0.20	🔒
2017-02-10	13G/A	ALLIANCEBERNSTEIN L.P.	↗	🔒	428,586	🔒	0.40	🔒
2016-02-12	13G/A	Capital World Investors	↗	🔒	500,000	🔒	0.50	🔒
2014-02-14	13G/A	RS INVESTMENT MANAGEMENT CO LLC	↗	🔒	0	🔒	0.00	🔒
2014-01-28	13G/A	ROYCE & ASSOCIATES LP	↗	🔒	2,648,566	🔒	2.29	🔒
2012-02-14	13G/A	UBS ASSET MANAGEMENT AMERICAS INC	↗	🔒	6,545,856	🔒	4.80	🔒



File Date	Form	Investor		Opt	Avg Share Price	Shares	Shares Changed (%)	Value ($1000)	Value Changed (%)	Cost Basis (x1000)	Profit (x1000)	Return (%)
2021-01-29	NP	VCSVX - Small Cap Value Fund	↗		🔒	20,900	🔒	346	🔒	🔒	🔒	🔒
2021-01-27	NP	BIGTX - The Texas Fund Class I	↗		🔒	5,464	🔒	90	🔒	🔒	🔒	🔒
2021-01-27	NP	VCSLX - Small Cap Index Fund	↗		🔒	27,344	🔒	453	🔒	🔒	🔒	🔒
2021-01-27	13F	Tarbox Family Office, Inc.	↗		13.76	109	0.00	2	100.00	🔒	🔒	🔒
2021-01-27	13F	Cwm, Llc	↗		14.55	2,251	17.61	42	110.00	🔒	🔒	🔒
2021-01-27	13F	CenterStar Asset Management, LLC	↗	Put	🔒	🔒	🔒	🔒	🔒	🔒	🔒	🔒
2021-01-27	NP	GSSC - Goldman Sachs ActiveBeta(R) U.S. Small Cap Equity ETF	↗		🔒	12,171	🔒	202	🔒	🔒	🔒	🔒
2021-01-27	13F	CenterStar Asset Management, LLC	↗					36	-94.07	🔒	🔒	🔒
2021-01-26	NP	SCHA - Schwab U.S. Small-Cap ETF	↗		🔒	202,899	🔒	3,360	🔒	🔒	🔒	🔒
2021-01-26	13F	Hc Financial Advisors Inc	↗		0.00	5	0.00	0		🔒	🔒	🔒
2021-01-26	NP	FNDX - Schwab Fundamental U.S. Large Company Index ETF	↗		🔒	497,766	🔒	8,243	🔒	🔒	🔒	🔒
2021-01-26	NP	SCHB - Schwab U.S.	↗		🔒	27,155	🔒	450	🔒	🔒	🔒	🔒

Passwords, recap from L3

Breaking Hashed Passwords

- **Stored passwords should always be salted**
  - Forces the attacker to brute-force each password individually

Breaking Hashed Passwords

- **Stored passwords should always be salted**
  - Forces the attacker to brute-force each password individually
- Problem: it is now possible to compute hashes very quickly
  - GPU computing: hundreds of small CPU cores
  - nVidia GeForce GTX Titan Z: 5,760 cores
  - GPUs can be rented from the cloud very cheaply
    - $0.9 per hour (2018 prices)

Examples of Hashing Speed

- A modern x86 server can hash all possible 6 character long passwords in 3.5 hours
  - Upper and lowercase letters, numbers, symbols
  - $(26+26+10+32)^6$ = 690 billion combinations

Examples of Hashing Speed

- A modern x86 server can hash all possible 6 character long passwords in 3.5 hours
  - Upper and lowercase letters, numbers, symbols
  - $(26+26+10+32)^6$ = 690 billion combinations
- A modern GPU can do the same thing in 16 minutes

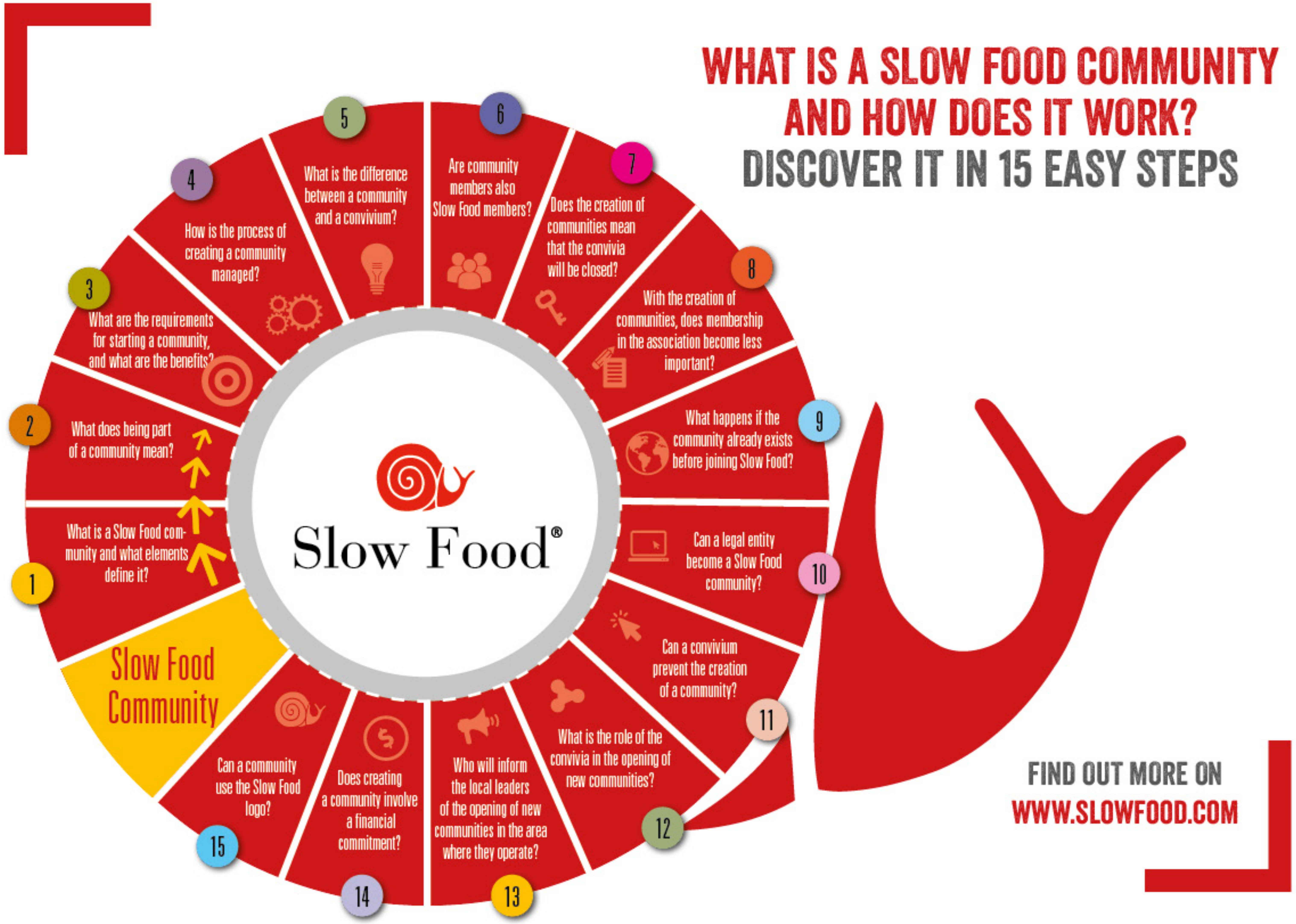
Examples of Hashing Speed

- A modern x86 server can hash all possible 6 character long passwords in 3.5 hours
  - Upper and lowercase letters, numbers, symbols
  - $(26+26+10+32)^6$ = 690 billion combinations
- A modern GPU can do the same thing in 16 minutes
- Most users use (slightly permuted) dictionary words, no symbols
  - Predictability makes cracking much faster
  - Lowercase + numbers → $(26+10)^6$ = 2B combinations

Hardening Salted Passwords

- Problem: typical hashing algorithms are too fast
  - Enables GPUs to brute-force passwords
- Old solution: hash the password multiple times
  - Known as key stretching
  - Example: *crypt* used 25 rounds of DES
- New solution: use hash functions that are designed to be **slow**
  - Examples: bcrypt, PBKDF2, scrypt
  - These algorithms include a work factor that increases the time complexity of the calculation
  - scrypt also requires a large amount of memory to compute, further complicating brute-force attacks

Slow hash movement



WHAT IS A SLOW FOOD COMMUNITY AND HOW DOES IT WORK?

DISCOVER IT IN 15 EASY STEPS

Slow Food®

Slow Food Community

1 What is a Slow Food community and what elements define it?

2 What does being part of a community mean?

3 What are the requirements for starting a community, and what are the benefits?

4 How is the process of creating a community managed?

5 What is the difference between a community and a convivium?

6 Are community members also Slow Food members?

7 Does the creation of communities mean that the convivia will be closed?

8 With the creation of communities, does membership in the association become less important?

9 What happens if the community already exists before joining Slow Food?

10 Can a legal entity become a Slow Food community?

11 Can a convivium prevent the creation of a community?

12 What is the role of the convivia in the opening of new communities?

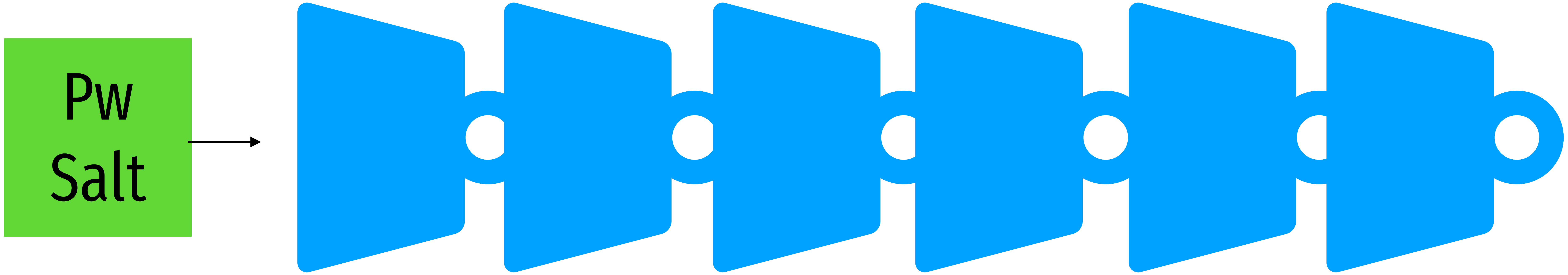
13 Who will inform the local leaders of the opening of new communities in the area where they operate?

14 Does creating a community involve a financial commitment?

15 Can a community use the Slow Food logo?

FIND OUT MORE ON WWW.SLOWFOOD.COM

Iterated hash function {x times}

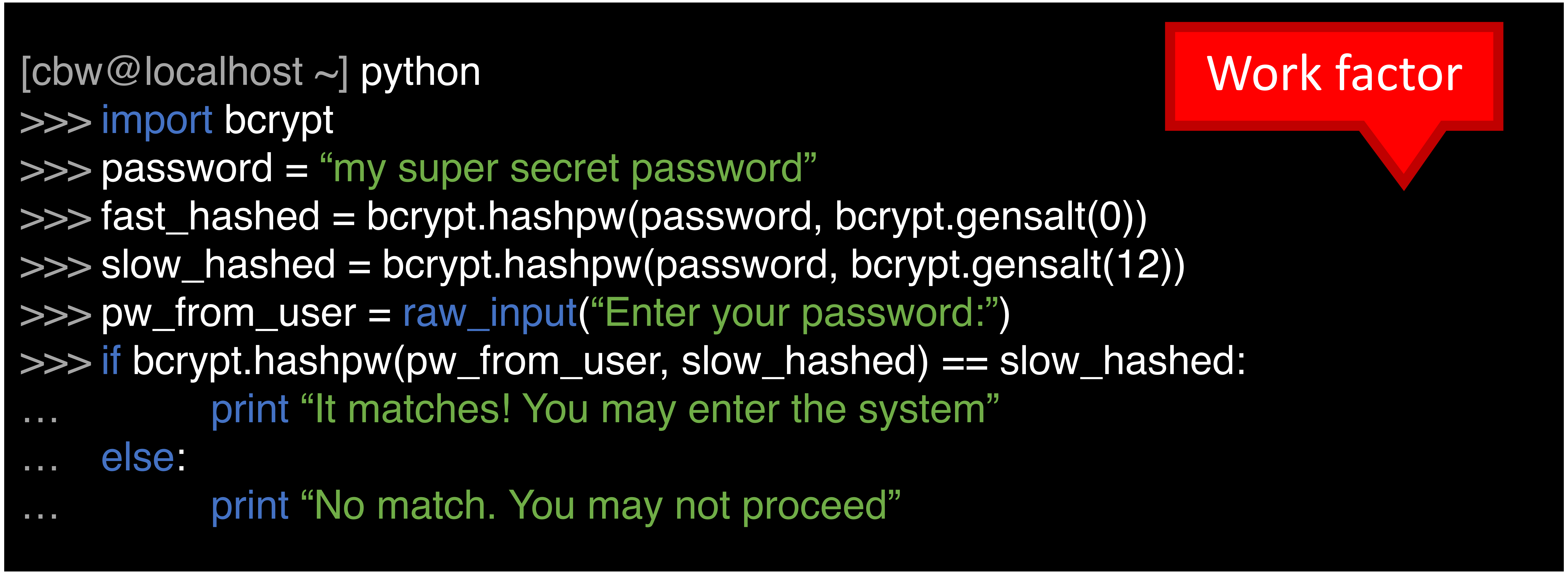


Pw
Salt

Hashed pwd

bcrypt Example

- Python example; install the *bcrypt* package



```
[cbw@localhost ~] python
>>> import bcrypt
>>> password = “my super secret password”
>>> fast_hashed = bcrypt.hashpw(password, bcrypt.gensalt(0))
>>> slow_hashed = bcrypt.hashpw(password, bcrypt.gensalt(12))
>>> pw_from_user = raw_input(“Enter your password:”)
>>> if bcrypt.hashpw(pw_from_user, slow_hashed) == slow_hashed:
…           print “It matches! You may enter the system”
…   else:
…           print “No match. You may not proceed”
```

Work factor

Best practices so far:

Dealing With Breaches

Dealing With Breaches

- Suppose you build an extremely secure password storage system
  - All passwords are salted and hashed by a high-work factor function
- It is still possible for a dedicated attacker to steal and crack passwords
  - Given enough time and money, anything is possible
  - E.g. The NSA
- Question: is there a principled way to detect password breaches?

Honeywords

- Key idea: store multiple salted/hashed passwords for each user
  - As usual, users create a single password and use it to login
  - User is unaware that additional honeywords are stored with their account

Honeywords

- Key idea: store multiple salted/hashed passwords for each user
  - As usual, users create a single password and use it to login
  - User is unaware that additional honeywords are stored with their account
- Implement a honeyserver that stores the index of the correct password for each user
  - Honeyserver is logically and physically separate from the password database
  - Silently checks that users are logging in with true passwords, not honeywords

Honeywords

- Key idea: store multiple salted/hashed passwords for each user
  - As usual, users create a single password and use it to login
  - User is unaware that additional honeywords are stored with their account
- Implement a honeyserver that stores the index of the correct password for each user
  - Honeyserver is logically and physically separate from the password database
  - Silently checks that users are logging in with true passwords, not honeywords
- What happens after a data breach?
  - Attacker dumps the user/password database…
  - But the attacker doesn't know which passwords are honeywords
  - Attacker cracks all passwords and uses them to login to accounts
  - If the attacker logs-in with a honeyword, the honeyserver raises an alert!

Honeywords example

Database

User	Salt 1	H(PW 1)	Salt 2	H(PW 2)	Salt 3	H(PW 3)
Bob	aB	y4DvF7	fl	bHDJ8l	52	Puu2s7
sandi	0x	plDS4F	K2	R/p3Y8	8W	S8x4Gk
Alice	9j	0F3g5H	/s	03d5jW	cV	1sRbJ5

Honeyserver

User	Index
Bob	2
sandi	3
Alice	1

Honeywords example

Bob

Database

User	Salt 1	H(PW 1)	Salt 2	H(PW 2)	Salt 3	H(PW 3)
Bob	aB	y4DvF7	fl	bHDJ8l	52	Puu2s7
sandi	0x	plDS4F	K2	R/p3Y8	8W	S8x4Gk
Alice	9j	0F3g5H	/s	03d5jW	cV	1sRbJ5

Honeyserver

User	Index
Bob	2
sandi	3
Alice	1

Honeywords example

Bob

SHA512(“fl” | “p4ssW0rd”) → bHDJ8l

Database

User	Salt 1	H(PW 1)	Salt 2	H(PW 2)	Salt 3	H(PW 3)
Bob	aB	y4DvF7	fl	bHDJ8l	52	Puu2s7
sandi	0x	plDS4F	K2	R/p3Y8	8W	S8x4Gk
Alice	9j	0F3g5H	/s	03d5jW	cV	1sRbJ5

Honeyserver

User	Index
Bob	2
sandi	3
Alice	1

Honeywords example

Bob

SHA512(“fl” | “p4ssW0rd”) → bHDJ8l

Database

User	Salt 1	H(PW 1)	Salt 2	H(PW 2)	Salt 3	H(PW 3)
Bob	aB	y4DvF7	fl	bHDJ8l	52	Puu2s7
sandi	0x	plDS4F	K2	R/p3Y8	8W	S8x4Gk
Alice	9j	0F3g5H	/s	03d5jW	cV	1sRbJ5

Honeyserver

User	Index
Bob	2
sandi	3
Alice	1

Honeywords example

Bob

SHA512(“fl” | “p4ssW0rd”) → bHDJ8l

Database

User	Salt 1	H(PW 1)	Salt 2	H(PW 2)	Salt 3	H(PW 3)
Bob	aB	y4DvF7	fl	bHDJ8l	52	Puu2s7
sandi	0x	plDS4F	K2	R/p3Y8	8W	S8x4Gk
Alice	9j	0F3g5H	/s	03d5jW	cV	1sRbJ5

Honeyserver

User	Index
Bob	2
sandi	3
Alice	1

Honeywords example

Bob

SHA512("fl" | "p4ssW0rd") → bHDJ8l

Cracked Passwords

User	PW 1	PW 2	PW 3
Bob	123456	p4ssW0rd	Turtles!
sandi	puppies	iloveyou	blizzard
Alice	coff33	3spr3ss0	qwerty

Database

User	Salt 1	H(PW 1)	Salt 2	H(PW 2)	Salt 3	H(PW 3)
Bob	aB	y4DvF7	fl	bHDJ8l	52	Puu2s7
sandi	0x	plDS4F	K2	R/p3Y8	8W	S8x4Gk
Alice	9j	0F3g5H	/s	03d5jW	cV	1sRbJ5

Honeyserver

User	Index
Bob	2
sandi	3
Alice	1

Honeywords example

Bob

SHA512(“fI” | “p4ssW0rd”) → bHDJ8l

Cracked Passwords

User	PW 1	PW 2	PW 3
Bob	123456	p4ssW0rd	Turtles!
sandi	puppies	iloveyou	blizzard
Alice	coff33	3spr3ss0	qwerty

Database

User	Salt 1	H(PW 1)	Salt 2	H(PW 2)	Salt 3	H(PW 3)
Bob	aB	y4DvF7	fI	bHDJ8l	52	Puu2s7
sandi	0x	pIDS4F	K2	R/p3Y8	8W	S8x4Gk
Alice	9j	0F3g5H	/s	03d5jW	cV	1sRbJ5

Honeyserver

User	Index
Bob	2
sandi	3
Alice	1

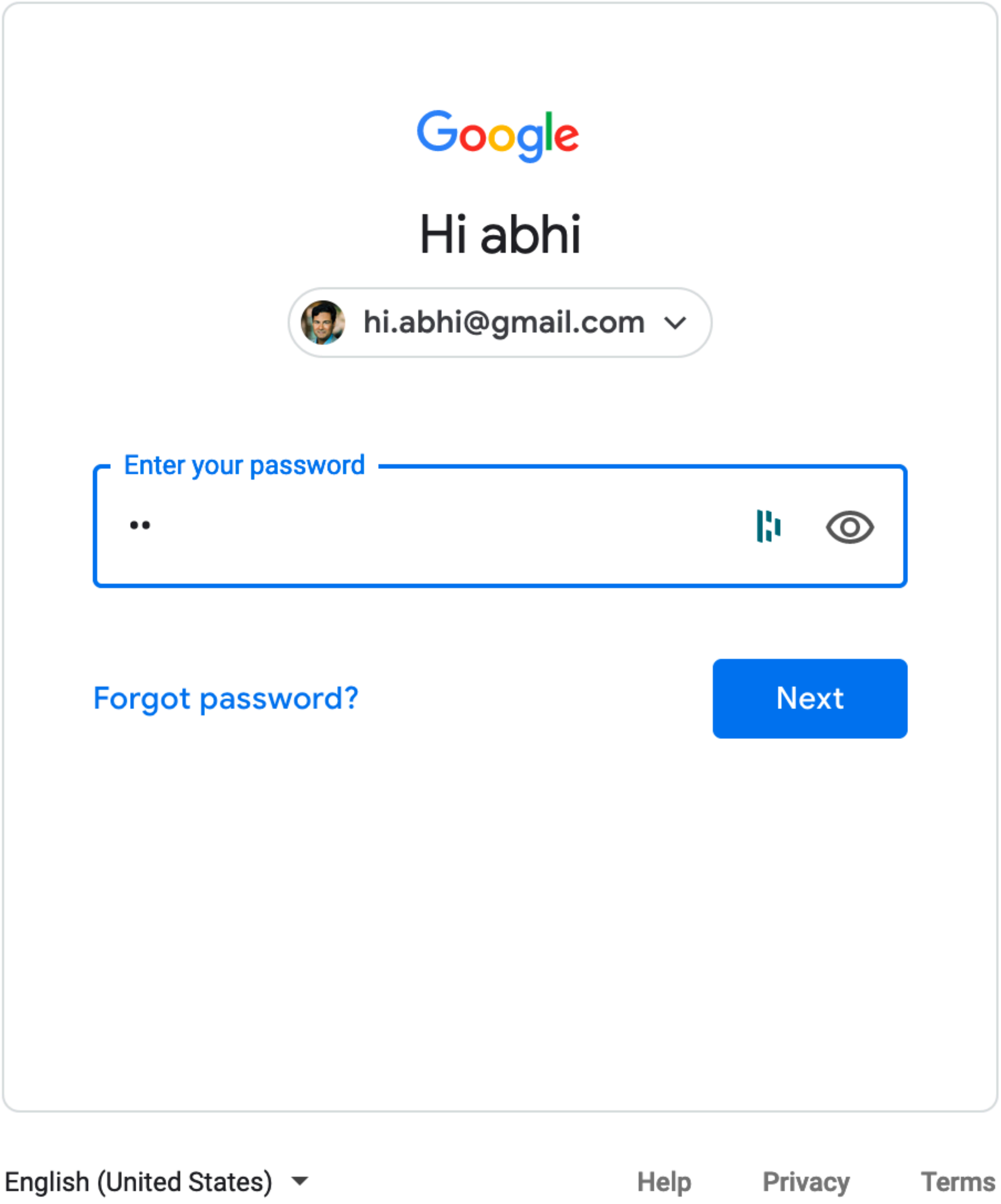
Multiple layers of storage

Password Storage Summary

1. **Never store passwords in plain text**
2. **Always salt and hash passwords before storing them**
3. **Use hash functions with a high work factor**
4. **Implement honeywords to detect breaches**

- These rules apply to any system that needs to authenticate users
  - Operating systems, websites, etc.

Still one problem?



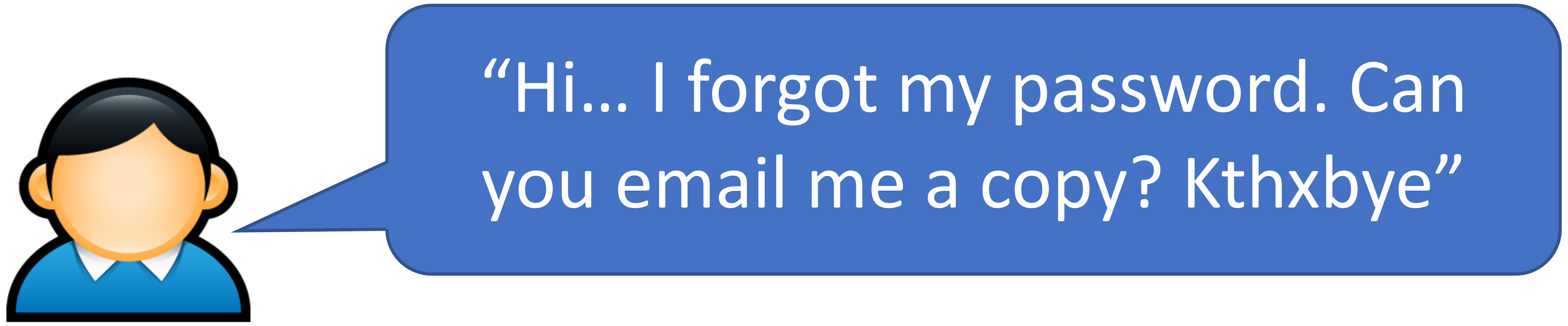
Hi abhi

hi.abhi@gmail.com

Enter your password: ••

Password Recovery/Reset

- Problem: hashed passwords cannot be recovered (hopefully)


"Hi… I forgot my password. Can you email me a copy? Kthxbye"

- This is why systems typically implement password reset
  - Use out-of-band info to authenticate the user
  - Overwrite hash(old_pw) with hash(new_pw)
- Be careful: its possible to crack password reset

Cracking Password Reset

- Typical implementations use Knowledge Based Authentication (KBA)
  - What was your mother’s maiden name?
  - What was your prior street address?
  - Where did you go to elementary school

Cracking Password Reset

- Typical implementations use Knowledge Based Authentication (KBA)
  - What was your mother’s maiden name?
  - What was your prior street address?
  - Where did you go to elementary school
- Problems?

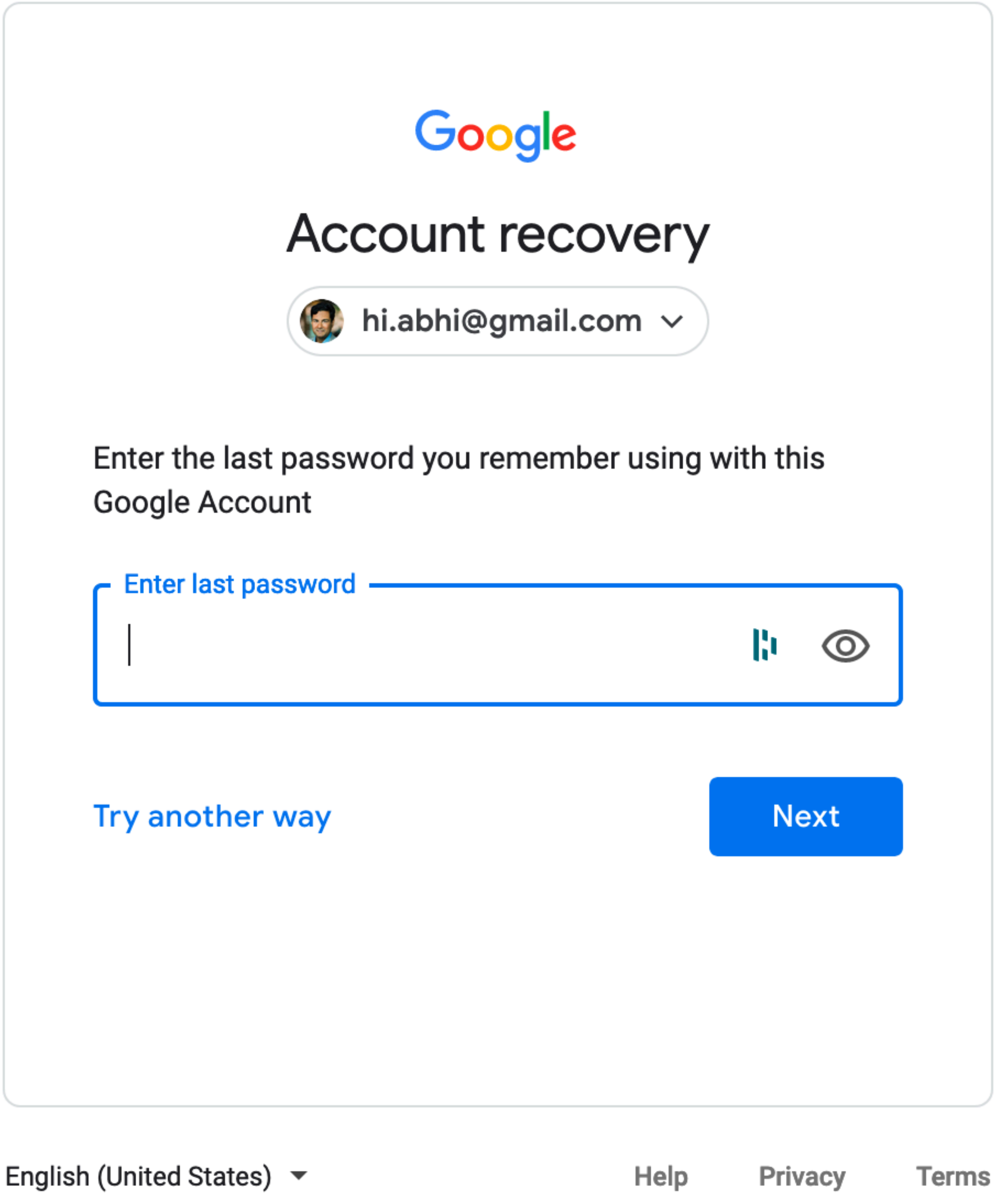
Cracking Password Reset

- Typical implementations use Knowledge Based Authentication (KBA)
  - What was your mother's maiden name?
  - What was your prior street address?
  - Where did you go to elementary school
- Problems?
  - This information is widely available to anyone
  - Publicly accessible social network profiles
  - Background-check services like Spokeo

Cracking Password Reset

- Typical implementations use Knowledge Based Authentication (KBA)
    - What was your mother's maiden name?
    - What was your prior street address?
    - Where did you go to elementary school
- Problems?
    - This information is widely available to anyone
    - Publicly accessible social network profiles
    - Background-check services like Spokeo
- Experts recommend that services not use KBA
    - When asked, users should generate random answers to these questions

Other roots of identity



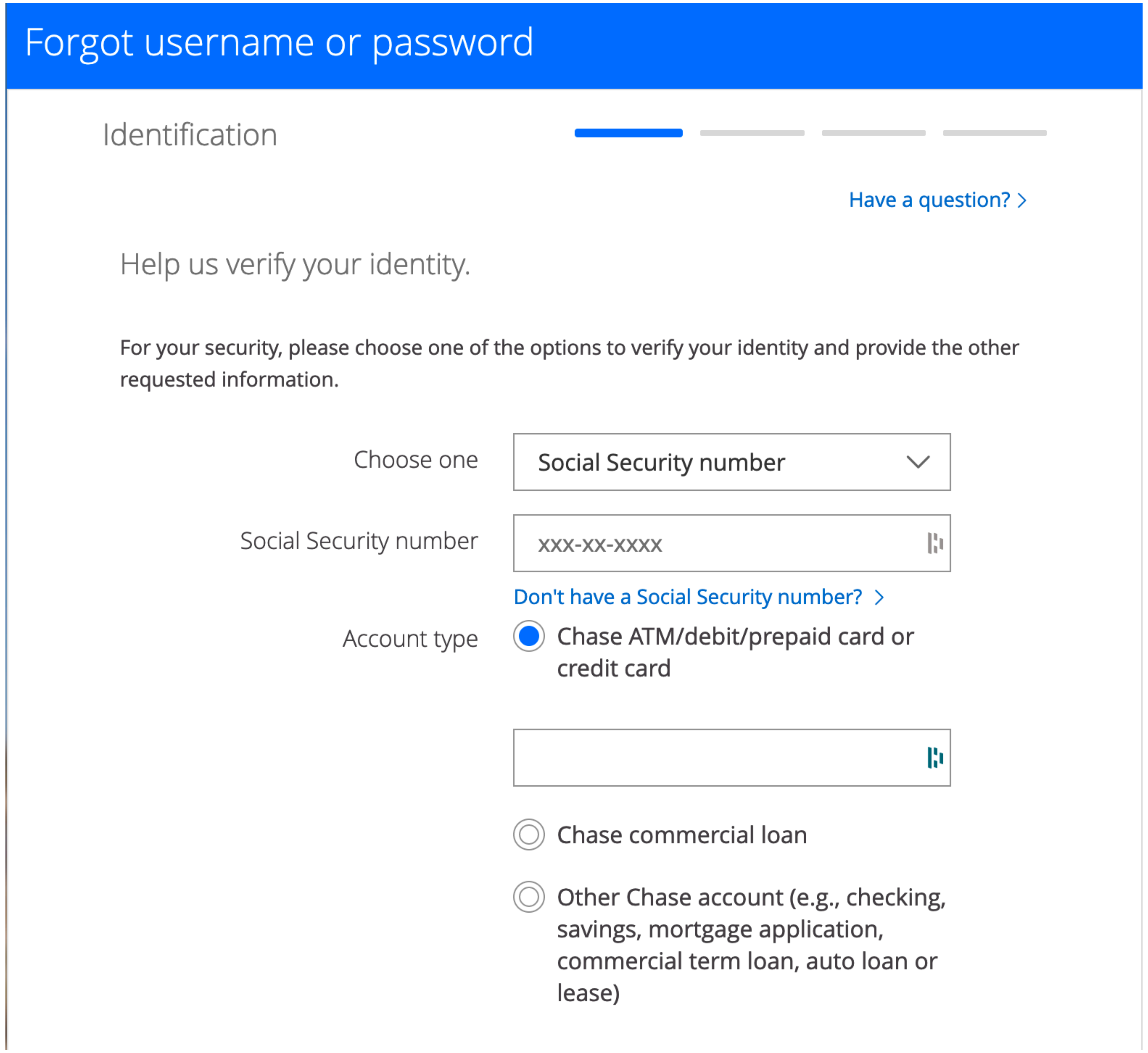
Google

Account recovery

hi.abhi@gmail.com

Enter the last password you remember using with this Google Account

Enter last password



Forgot username or password

Identification

Help us verify your identity.

For your security, please choose one of the options to verify your identity and provide the other requested information.

Choose one: Social Security number

Social Security number: XXX-XX-XXXX

Account type

● Chase ATM/debit/prepaid card or credit card

○ Chase commercial loan

○ Other Chase account (e.g., checking, savings, mortgage application, commercial term loan, auto loan or lease)

Choosing Passwords

Bad Algorithms

Better Heuristics

Password Reuse

Password Reuse

- People have difficulty remembering >4 passwords
  - Thus, people tend to reuse passwords across services
  - What happens if any one of these services is compromised?
- Service-specific passwords are a beneficial form of compartmentalization
  - Limits the damage when one service is inevitably breaches
- Use a password manager
- Some service providers now check for password reuse
  - Forbid users from selecting passwords that have appeared in leaks

LastPass •••|
Search your vault
fan@lastpass.com
95%
Sort By: Folder (a-z)
Launch
Read Only • Shared Folder
+

Sites

Favorites (8)

AirBnB
fan@lastpass.com

Amazon
fan@lastpass.com

Best Buy
fan@lastpass.com

Dropbox
fan@lastpass.com

Evernote
fan@lastpass.com

Facebook
fan@lastpass.com

Pocket
fan@lastpass.com

Twitter
fan@lastpass.com

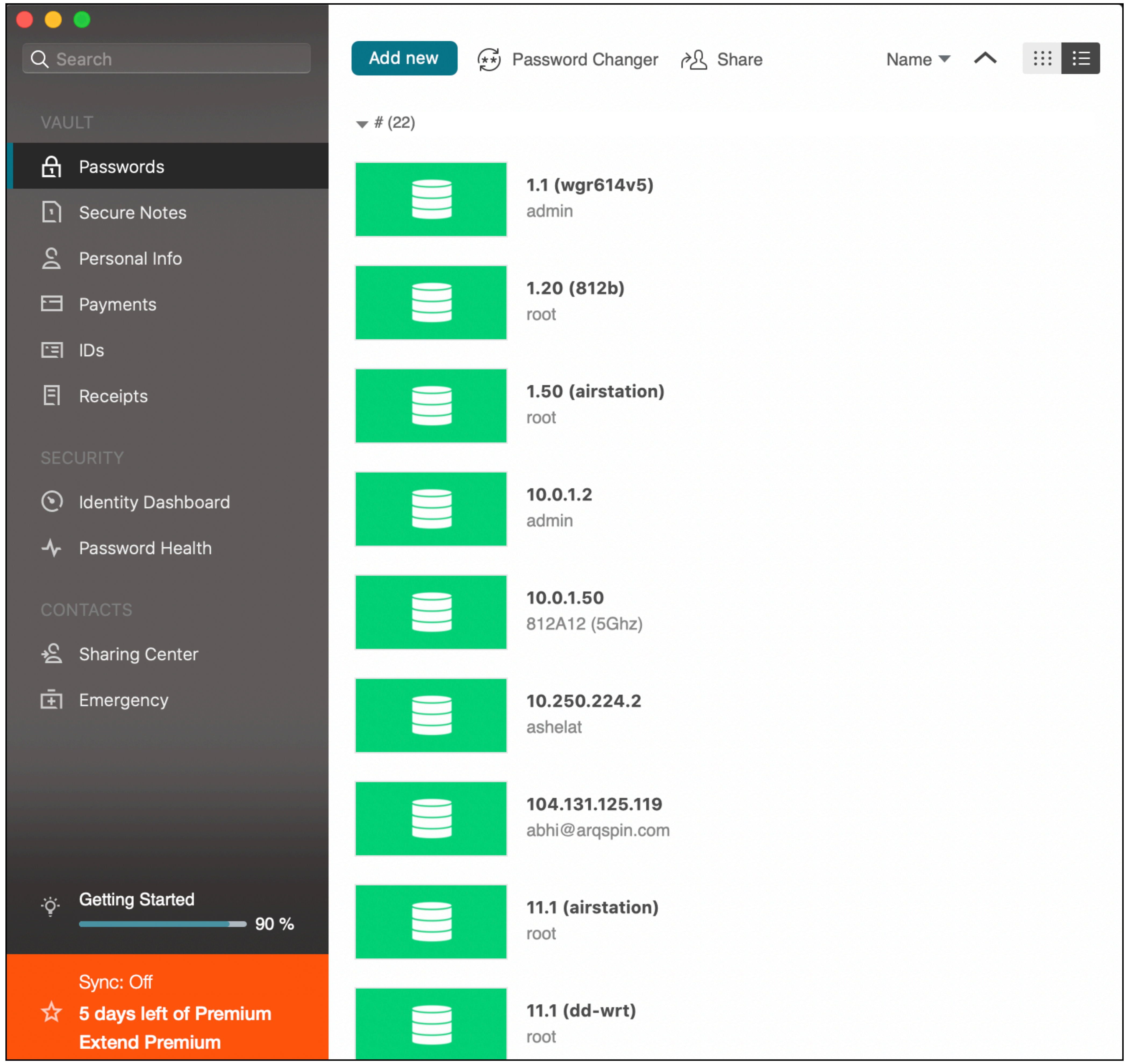
Banking and Finance (3)

Bank of America
fan@lastpass.com

Fidelity
fan@lastpass.com

Mint
fan@lastpass.com

Dashlane



(22)

1.1 (wgr614v5)
admin

1.20 (812b)
root

1.50 (airstation)
root

10.0.1.2
admin

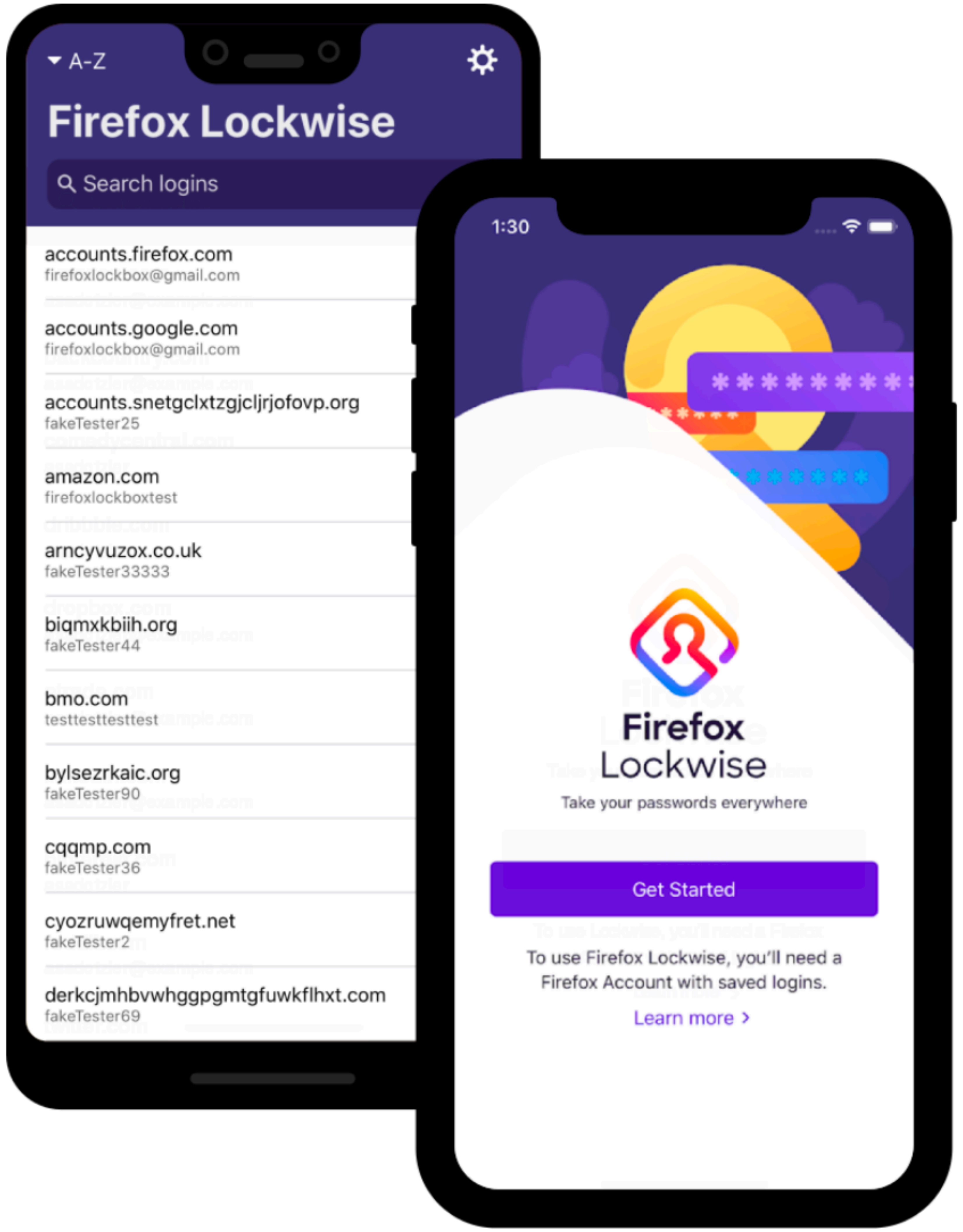
10.0.1.50
812A12 (5Ghz)

10.250.224.2
ashelat

104.131.125.119
abhi@arqspin.com

11.1 (airstation)
root

11.1 (dd-wrt)
root



accounts.firefox.com
firefoxlockbox@gmail.com

accounts.google.com
firefoxlockbox@gmail.com

accounts.snetgclxtzgjcljrjofovp.org
fakeTester25

amazon.com
firefoxlockboxtest

arncyvuzox.co.uk
fakeTester33333

biqmxkbiih.org
fakeTester44

bmo.com
testtesttesttest

bylsezrkaic.org
fakeTester90

cqqmp.com
fakeTester36

cyozruwqemyfret.net
fakeTester2

derkcjmhbvwhggpgmtgfuwkflhxt.com
fakeTester69

To use Firefox Lockwise, you'll need a Firefox Account with saved logins.

Have I Been Pwned (Troy Hunt) [AU]
https://haveibeenpwned.com
Upshot
Cooking
Homepage
Slack
';--
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
email address or username
pwned?

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

264
pwned websites

4,859,717,682
pwned accounts

61,081
pastes

59,268,789
paste accounts

Two Factor Authentication

Biometrics

SMS

Authentication Codes

Smartcards & Hardware Tokens

Types of Secrets

- Actors provide their secret to log-in to a system
- Three classes of secrets:
  1. Something you know
     - Example: a password
  2. Something you have
     - Examples: a smart card or smart phone
  3. Something you are
     - Examples: fingerprint, voice scan, iris scan

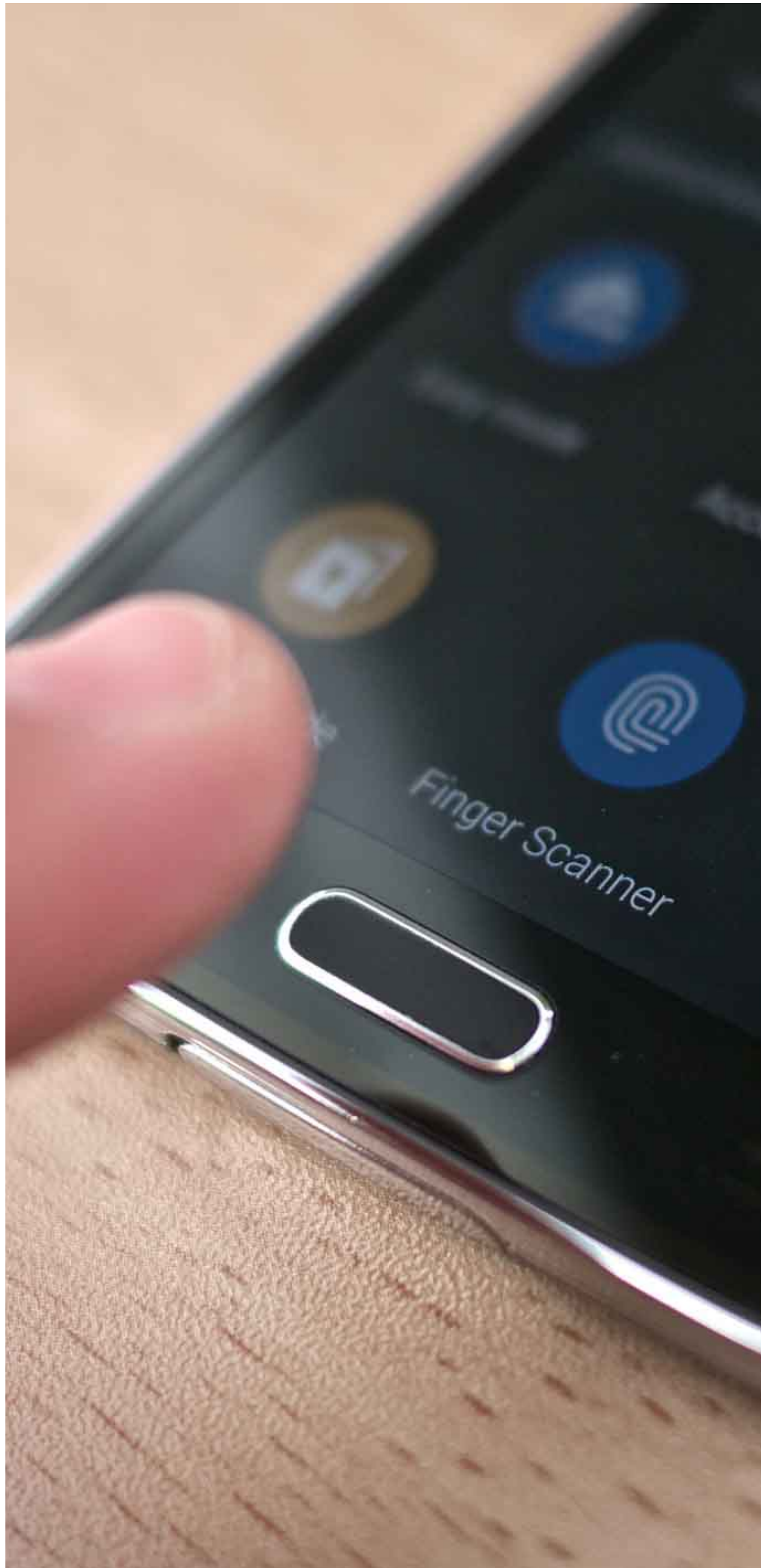
Biometrics

- ancient Greek: bios ="life", metron ="measure“
- Physical features
  - Fingerprints
  - Face recognition
  - Retinal and iris scans
  - Hand geometry
- Behavioral characteristics
  - Handwriting recognition
  - Voice recognition
  - Typing cadence
  - Gait

Fingerprints

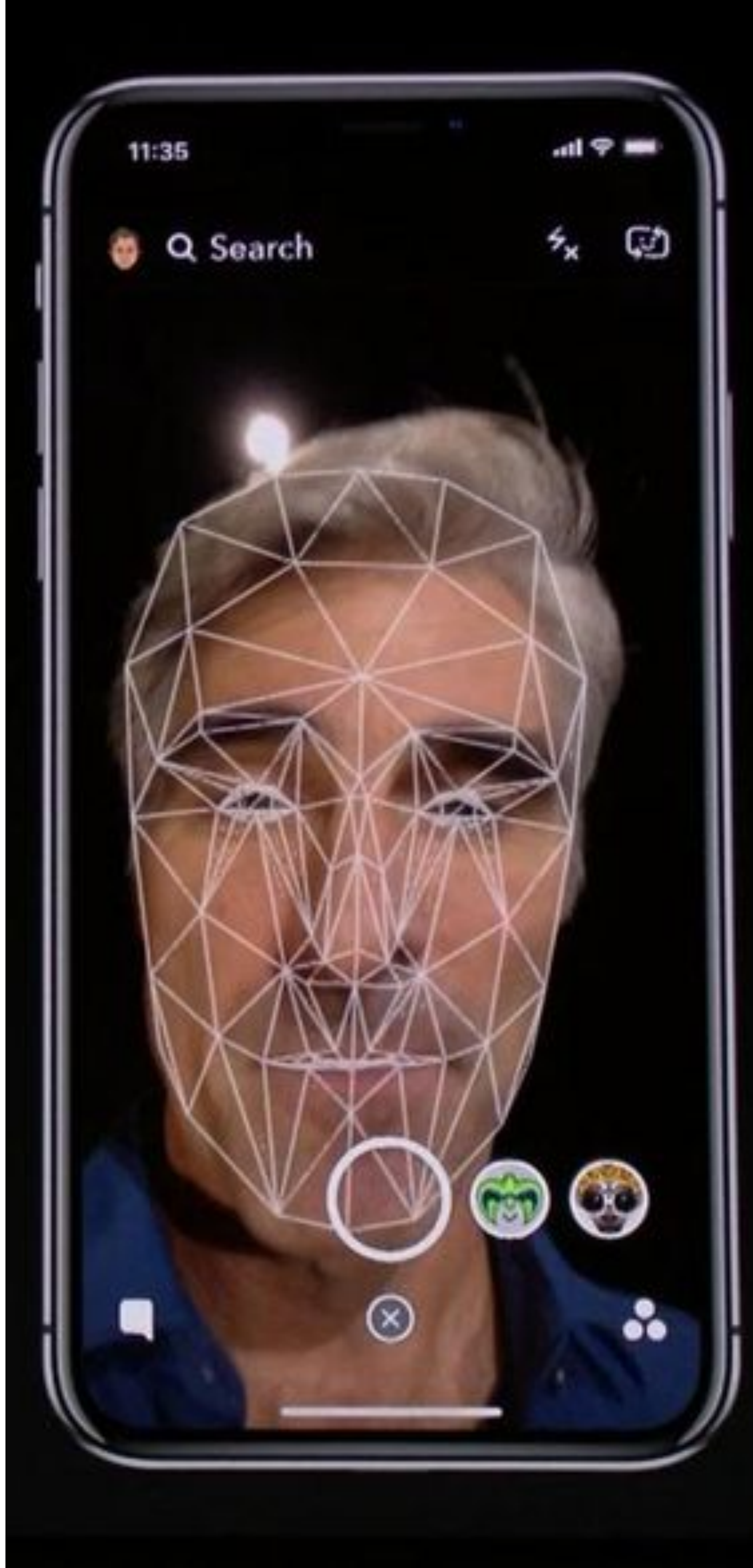
- Ubiquitous on modern smartphones, some laptops
- Secure?
  - May be subpoenaed by law enforcement
  - Relatively easy to compromise
    1. Pick up a latent fingerprint (e.g. off a glass) using tape or glue
    2. Photograph and enhance the fingerprint
    3. Etch the print into gelatin backed by a conductor
    4. Profit ;)

https://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/



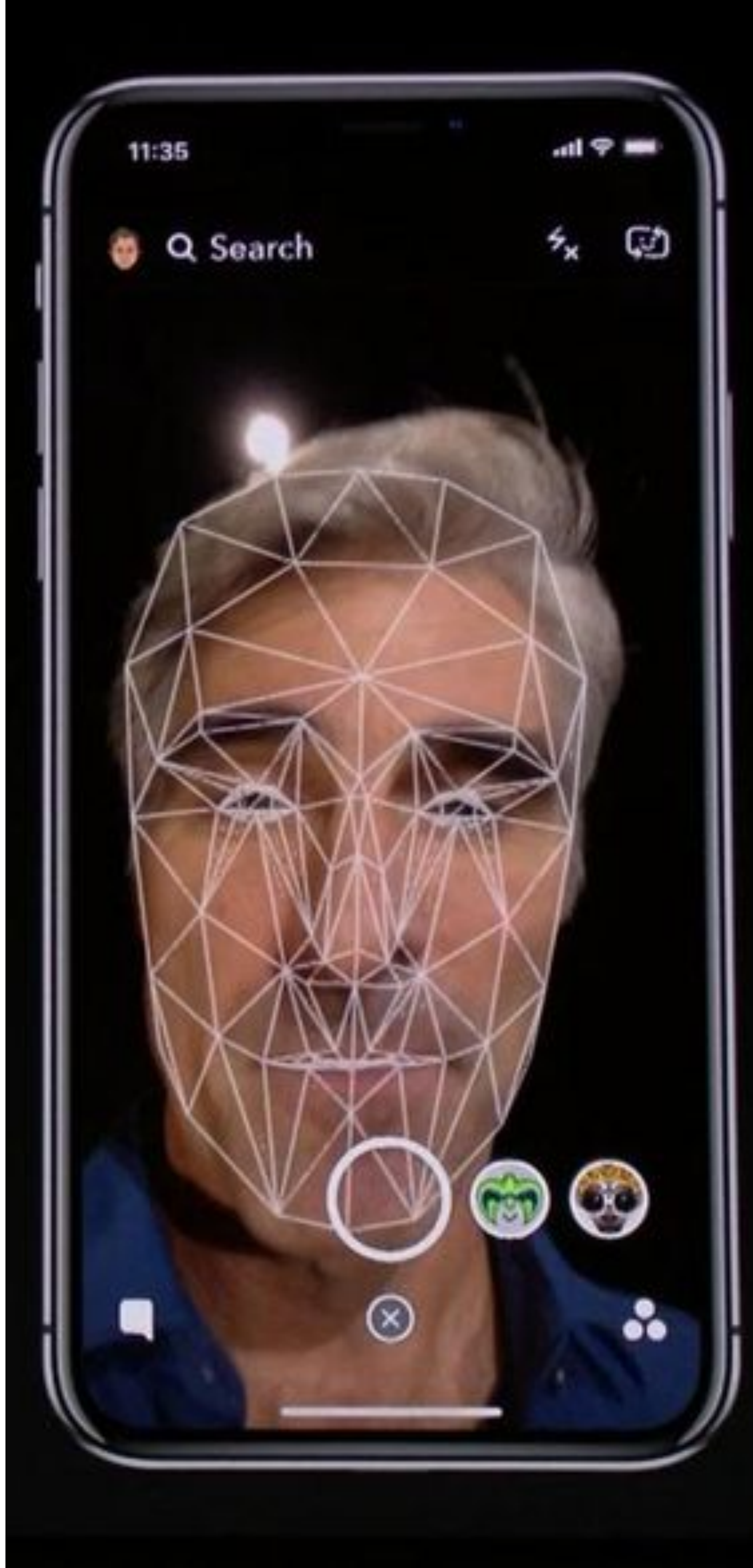
Facial Recognition

- Popularized by FaceID on the iPhone X
- Secure?



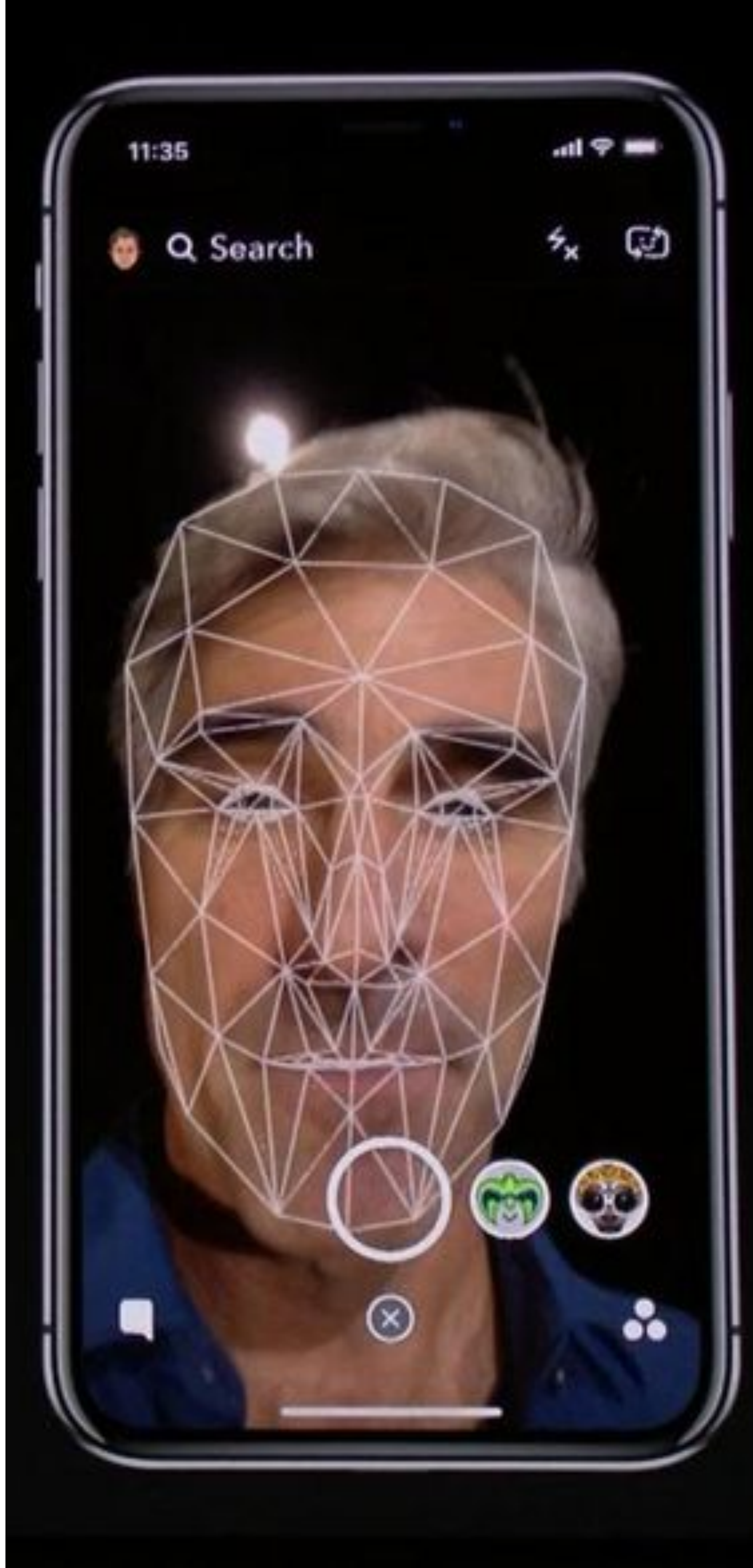
Facial Recognition

- Popularized by FaceID on the iPhone X
- Secure?
  - It depends



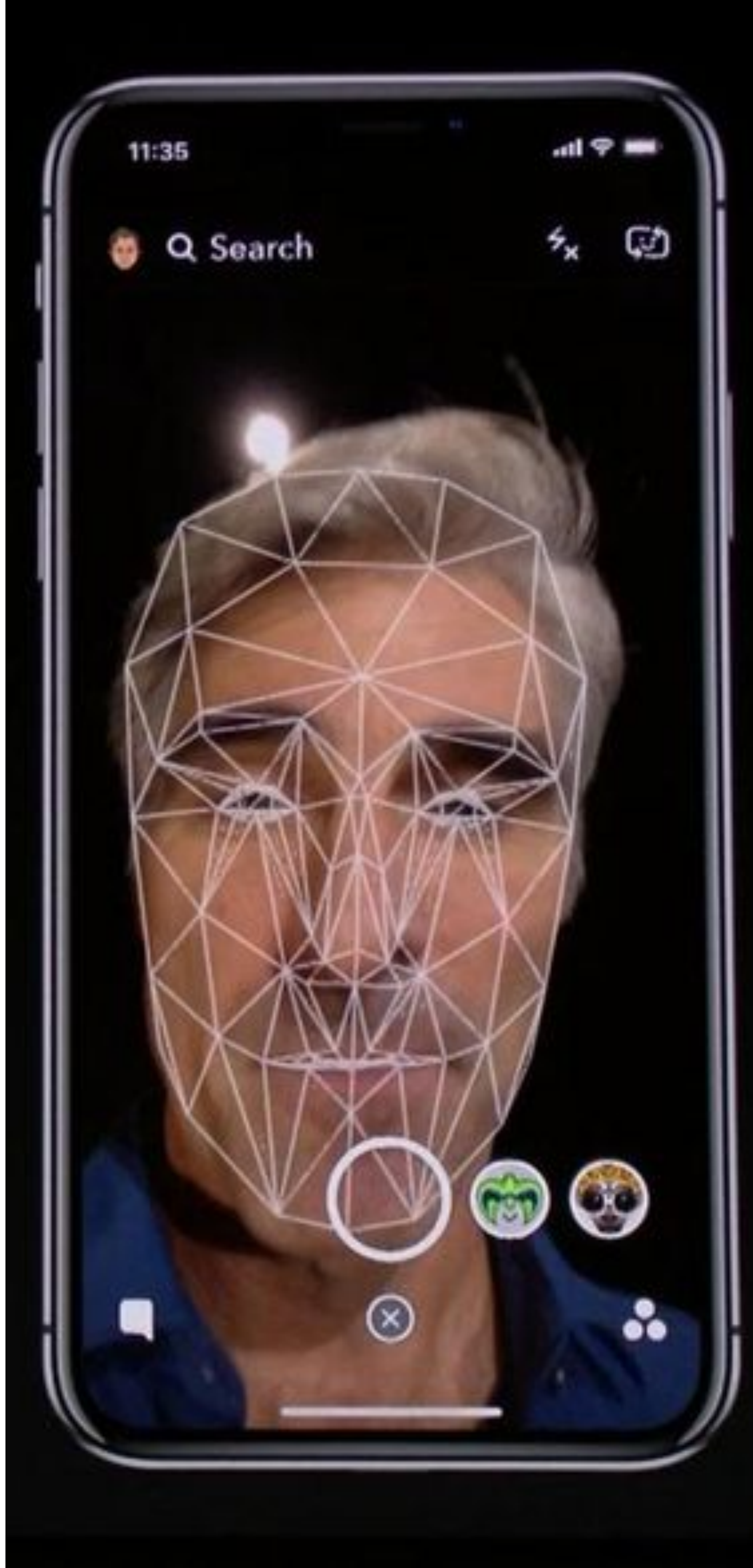
Facial Recognition

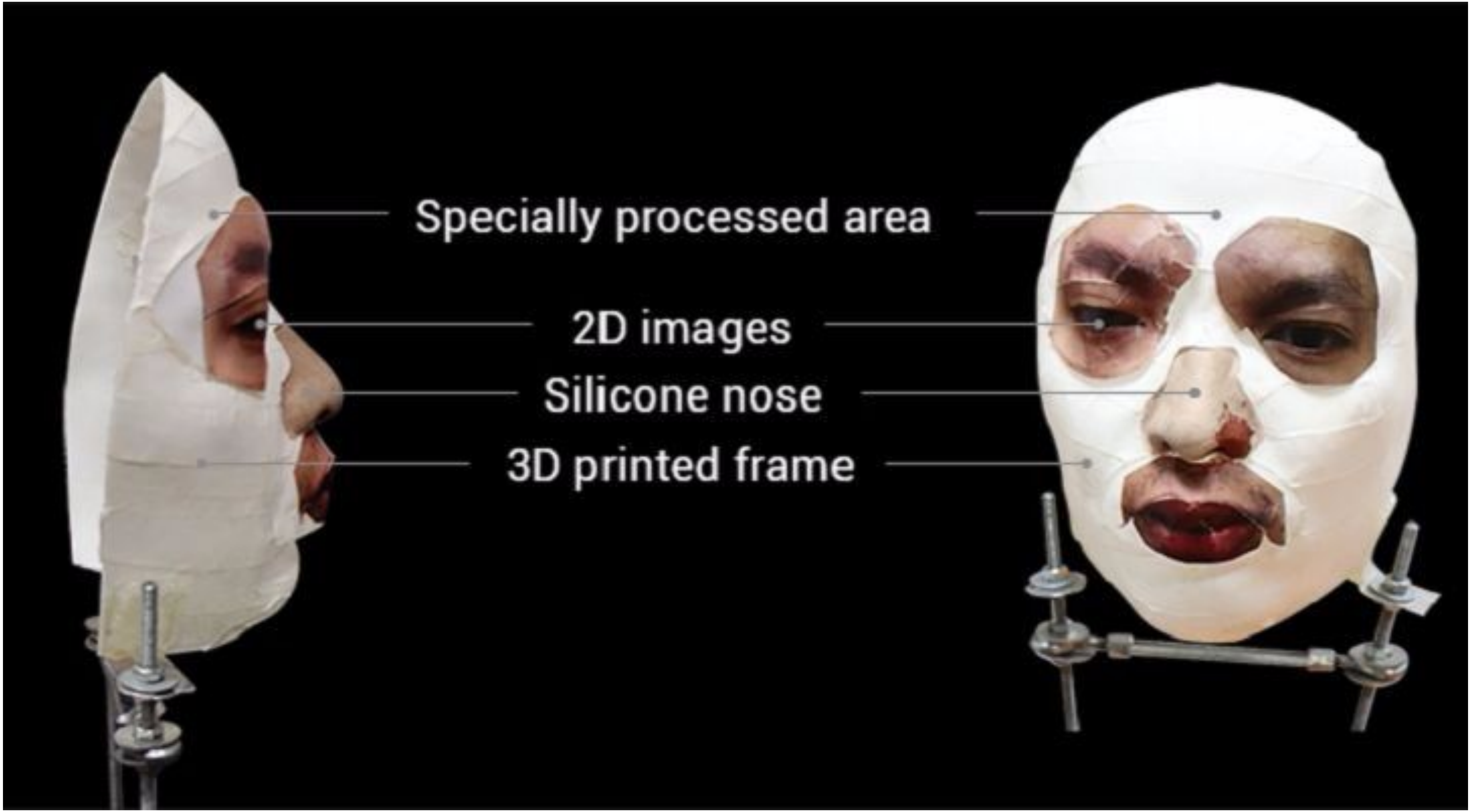
- Popularized by FaceID on the iPhone X
- Secure?
  - It depends
- Vulnerable to law enforcement requests
- Using 2D images?
  - Not secure
  - Trivial to break with a photo of the target’s face



Facial Recognition

- Popularized by FaceID on the iPhone X
- Secure?
  - It depends
- Vulnerable to law enforcement requests
- Using 2D images?
  - Not secure
  - Trivial to break with a photo of the target’s face
- Using 2D images + 3D depth maps?
  - More secure, but not perfect
  - Can be broken by crafting a lifelike mask of the target




Specially processed area
2D images
Silicone nose
3D printed frame

By Press Association

Saturday, October 19, 2019 - 01:20 PM

Google has confirmed the Face Unlock system on its new Pixel 4 smartphone can allow access to the device even when the user has their eyes closed.

Early testers of the phone, as well as security experts, have raised concerns it could lead to unauthorised access to the device.

It has been suggested someone else could gain access to the phone by holding it in front of the face of its sleeping owner, but Google said it meets security requirements.

The technology giant unveiled the new phone earlier this week.

In a statement, Google said: “Pixel 4 Face Unlock meets the security requirements as a strong biometric and can be used for payments and app authentication, including banking apps.

“It is resilient against unlock attempts via other means, like with masks.

“If you want to temporarily disable Face Unlock, you can use lockdown mode to temporarily require a PIN/pattern/password.

Voice Recognition

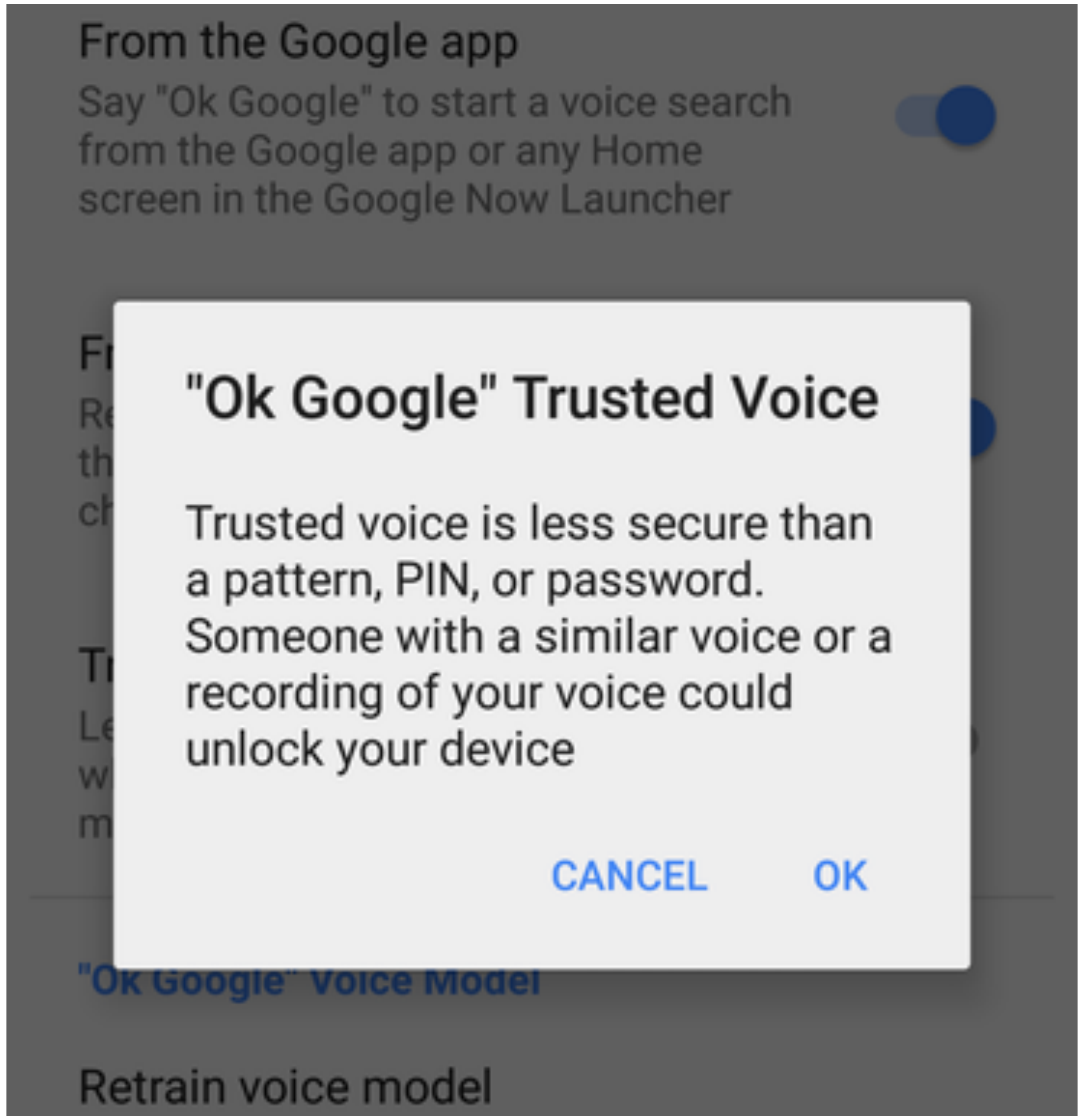
- Secure?
  - Very much depends on the implementation

Voice Recognition

- Secure?
  - Very much depends on the implementation
- Some systems ask you to record a static phrase
  - E.g. say “unlock” to unlock
  - This is wildly insecure
    - Attacker can record and replay your voice

Voice Recognition

- Secure?
  - Very much depends on the implementation
- Some systems ask you to record a static phrase
  - E.g. say “unlock” to unlock
  - This is wildly insecure
    - Attacker can record and replay your voice



From the Google app

Say "Ok Google" to start a voice search from the Google app or any Home screen in the Google Now Launcher

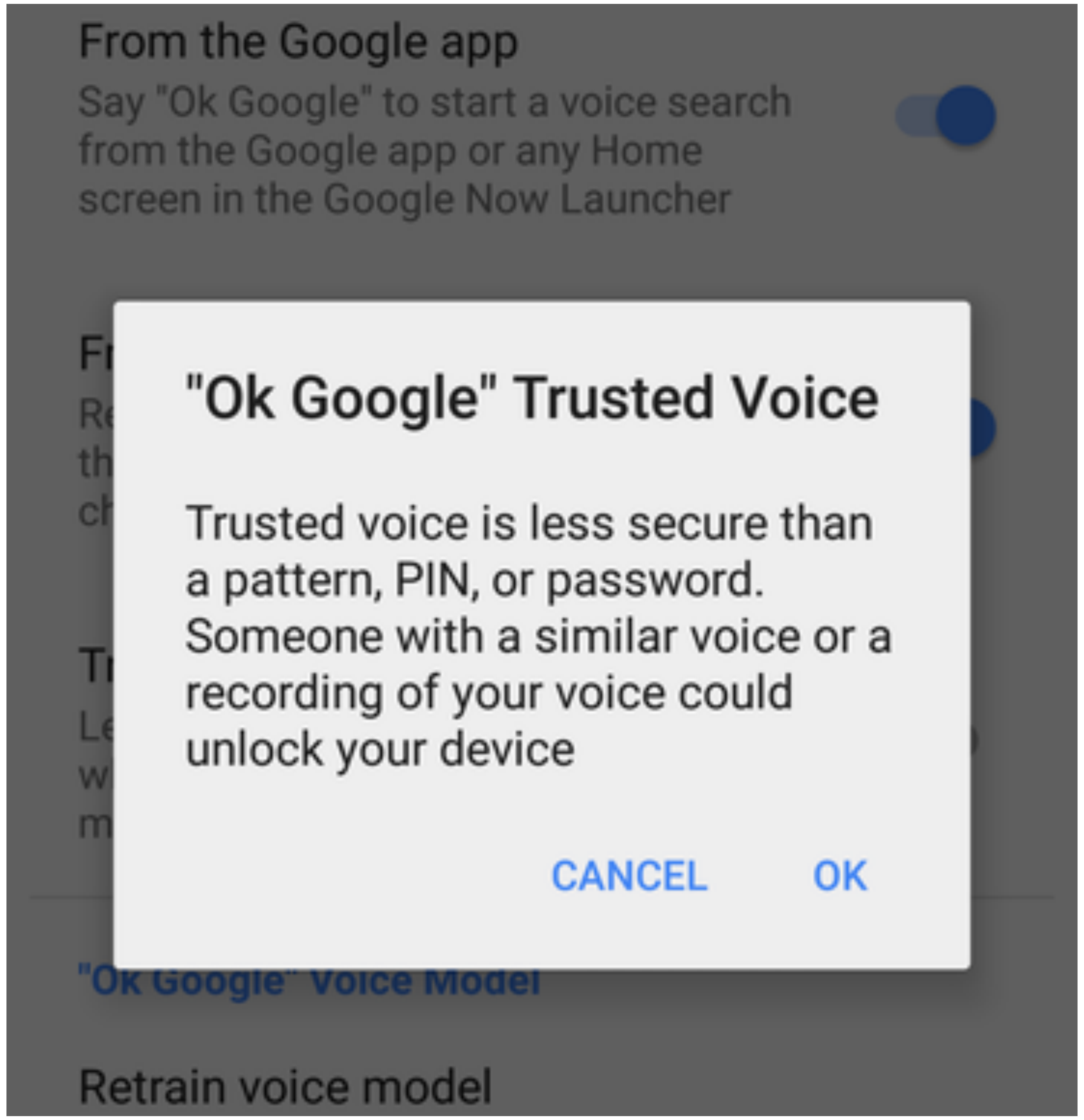
"Ok Google" Trusted Voice

Trusted voice is less secure than a pattern, PIN, or password. Someone with a similar voice or a recording of your voice could unlock your device

Retrain voice model

Voice Recognition

- Secure?
  - Very much depends on the implementation
- Some systems ask you to record a static phrase
  - E.g. say “unlock” to unlock
  - This is wildly insecure
    - Attacker can record and replay your voice
- Others ask you to train a model of your voice
  - Train the system by speaking several sentences
  - To authenticate, speak several randomly chosen words
  - Not vulnerable to trivial replay attacks, but still vulnerable
    - Given enough samples of your voice, an attacker can train a synthetic voice AI that sounds just like you



From the Google app

Say "Ok Google" to start a voice search from the Google app or any Home screen in the Google Now Launcher

"Ok Google" Trusted Voice

Trusted voice is less secure than a pattern, PIN, or password. Someone with a similar voice or a recording of your voice could unlock your device

"Ok Google" Voice Model

Retrain voice model

Fundamental Issue With Biometrics

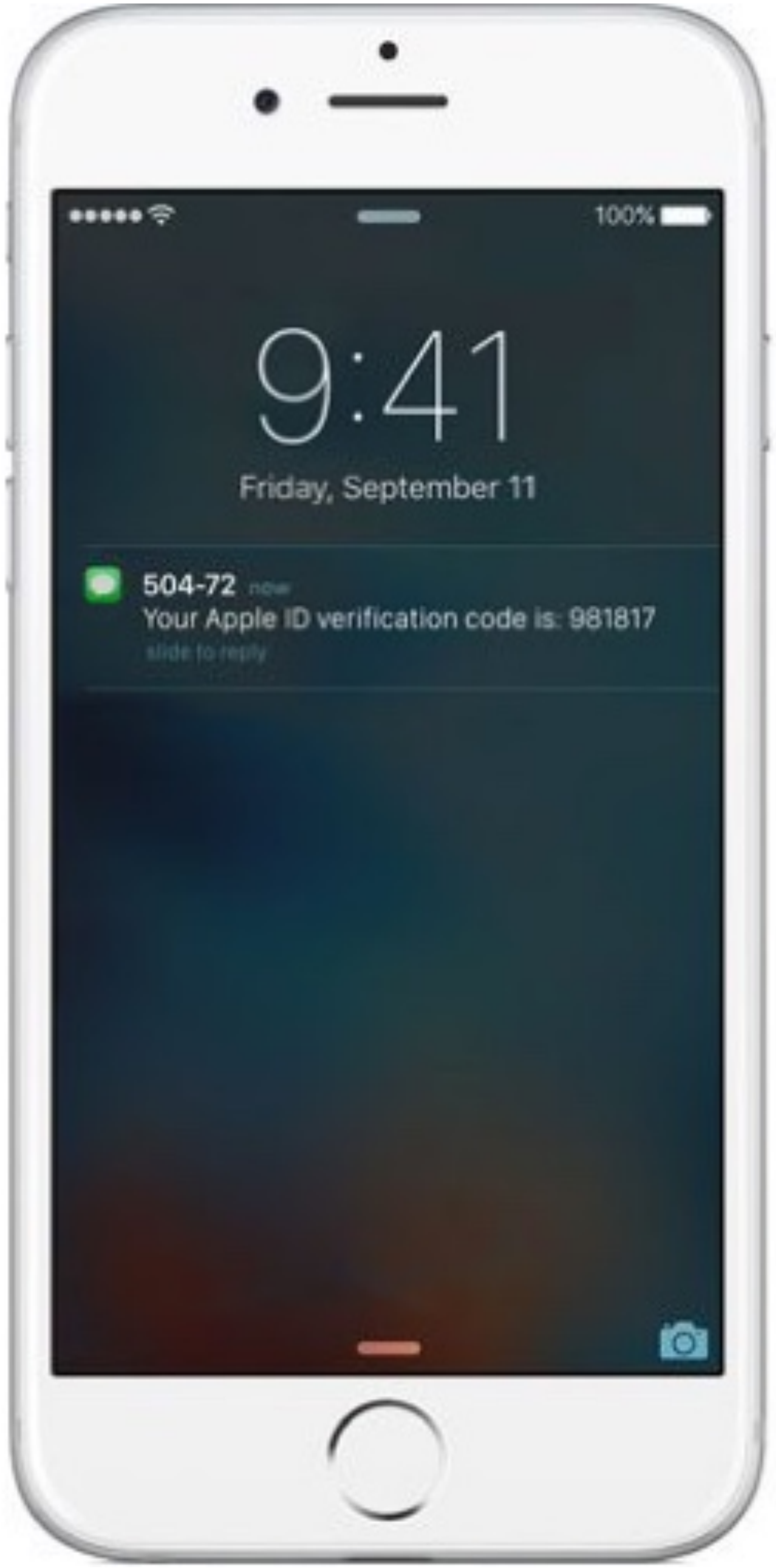
- Biometrics are immutable
  - You are the password, and you can’t change
  - Unless you plan on undergoing plastic surgery?
- Once compromised, there is no reset
  - Passwords and tokens can be changed
- Example: the Office of Personnel Management (OPM) breach
  - US gov agency responsible for background checks
  - Had fingerprint records of all people with security clearance
  - Breached by China in 2015, all records stolen :(

Something You Have

- Two-factor authentication has become more commonplace
- Possible second factors:
  - SMS passcodes
  - Time-based one time passwords
  - Hardware tokens

SMS Two Factor

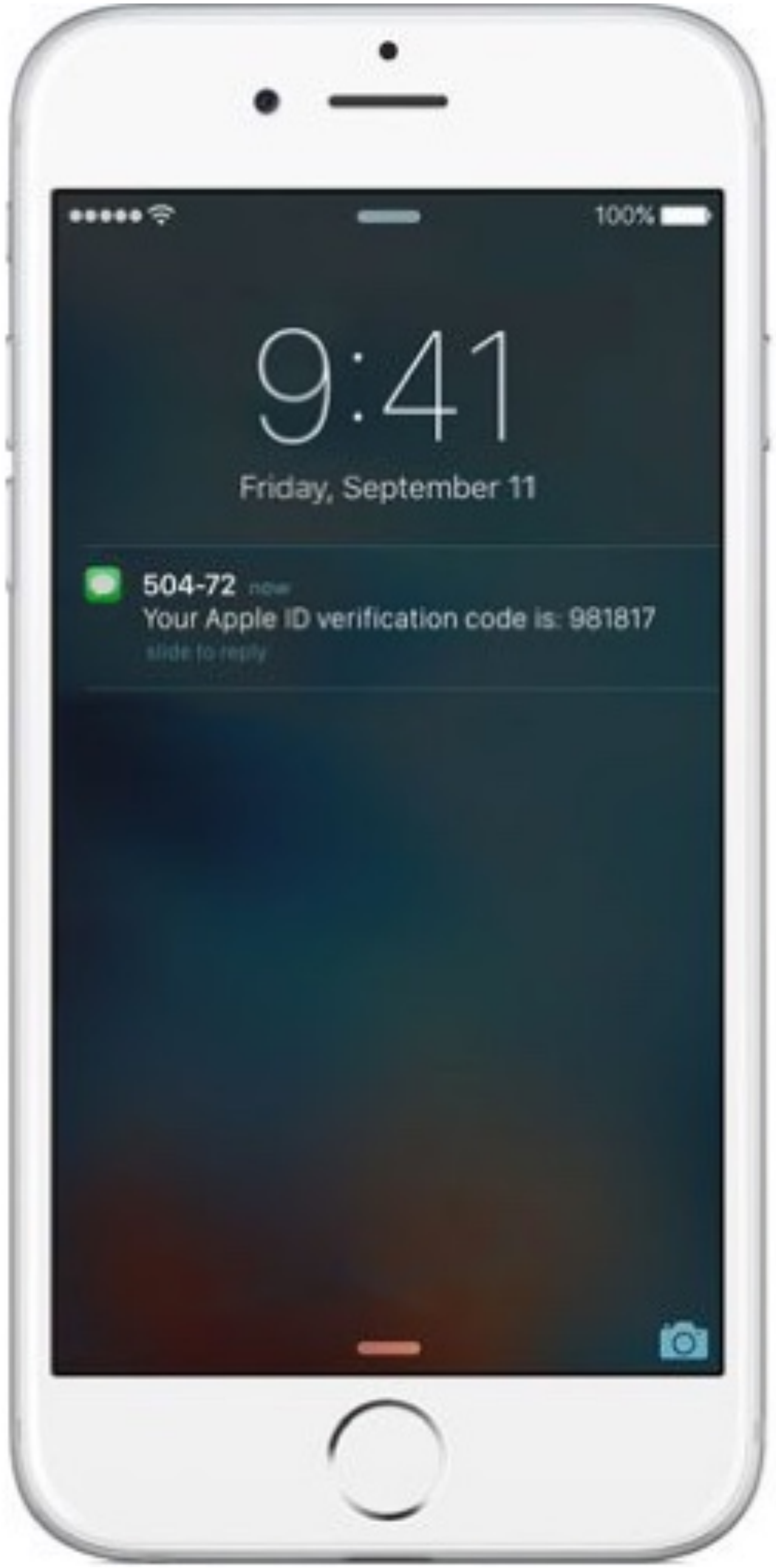
- Relies on your phone number as the second factor
  - Key assumption: only your phone should receive SMS sent to your number



504-72 now
Your Apple ID verification code is: 981817
slide to reply

SMS Two Factor

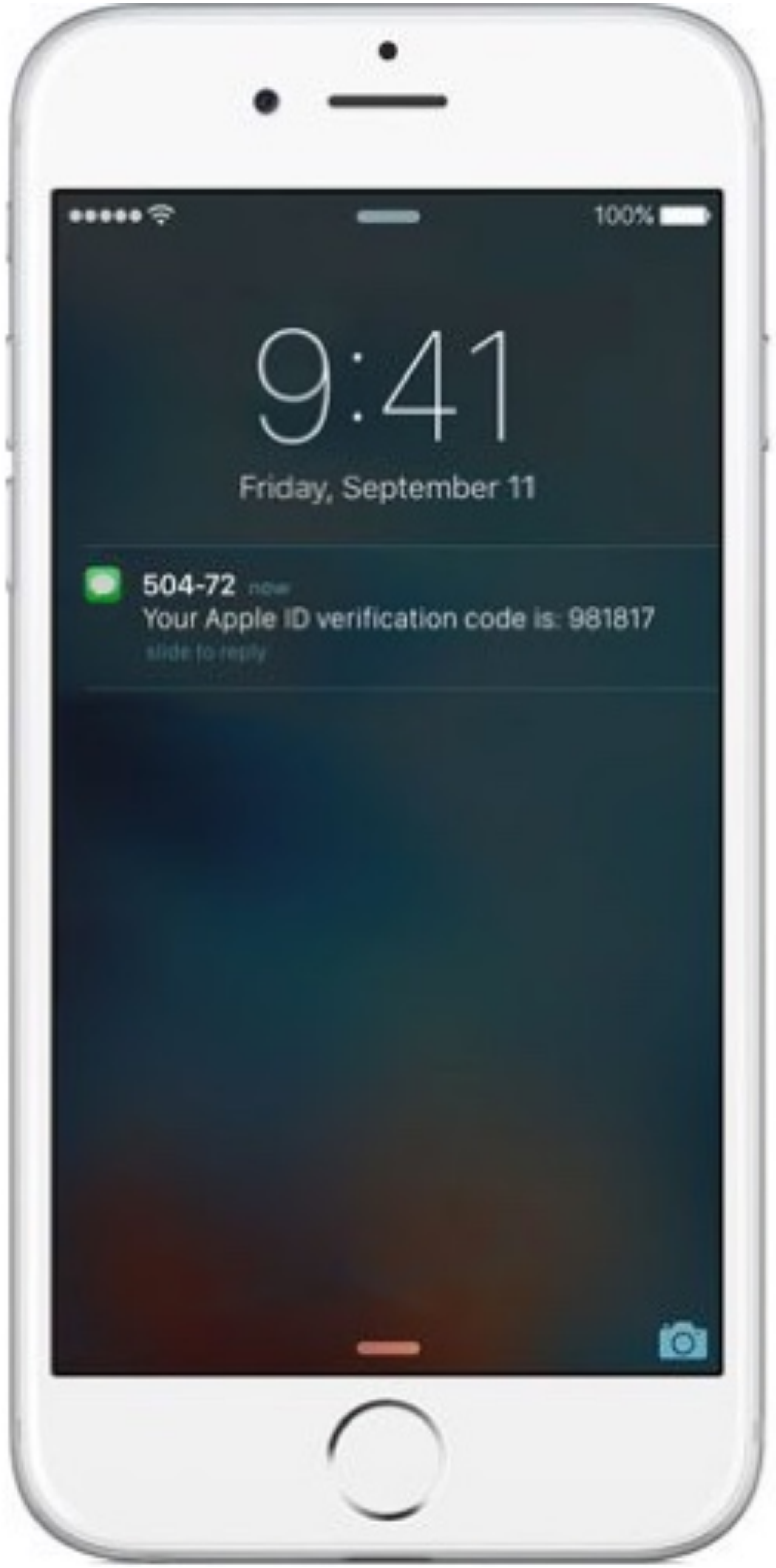
- Relies on your phone number as the second factor
  - Key assumption: only your phone should receive SMS sent to your number
- SMS two factor is deprecated. Why?



504-72 now
Your Apple ID verification code is: 981817
slide to reply

SMS Two Factor

- Relies on your phone number as the second factor
  - Key assumption: only your phone should receive SMS sent to your number
- SMS two factor is deprecated. Why?
- Social engineering the phone company
  1. Call and pretend to be the victim
  2. Say “I got a new SIM, please activate it”
  3. If successful, phone calls and SMS are now sent to your SIM in your phone, instead of the victim
- Not hypothetical: successfully used against many victims

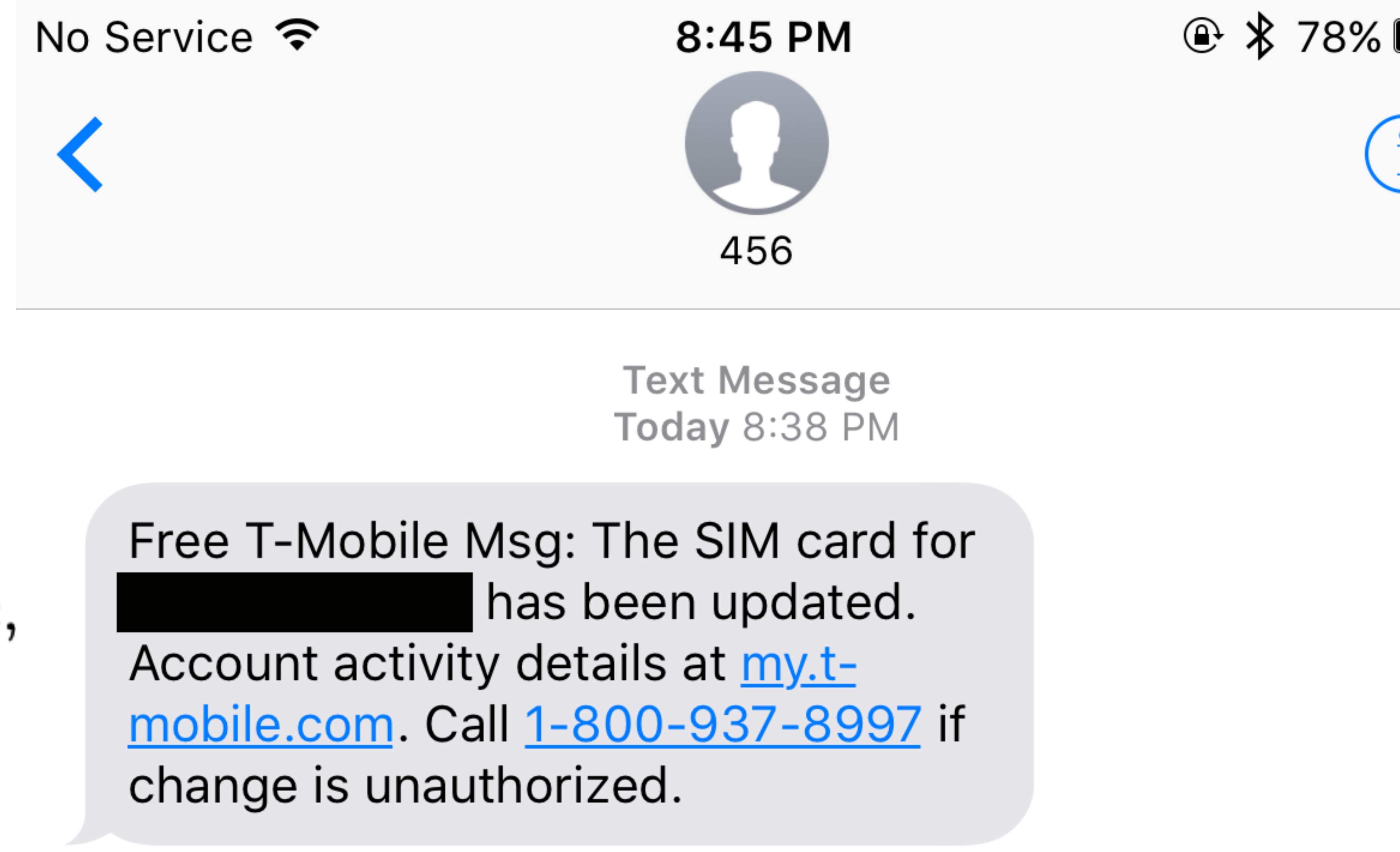


504-72 now
Your Apple ID verification code is: 981817
slide to reply

First, criminals call a cell phone carrier's tech support number pretending to be their target. They explain to the company's employee that they "lost" their SIM card, requesting their phone number be transferred, or ported, to a new SIM card that the hackers themselves already own. With a bit of social engineering—perhaps by providing the victim's Social Security Number or home address (which is often available from one of the many data breaches that have happened in the last few years)—the criminals convince the employee that they really are who they claim to be, at which point the employee ports the phone number to the new SIM card.

Game over.

"With someone's phone number," a hacker who does SIM swapping told me, "you can get into every account they own within minutes and they can't do anything about it."



Text Message
Today 8:38 PM

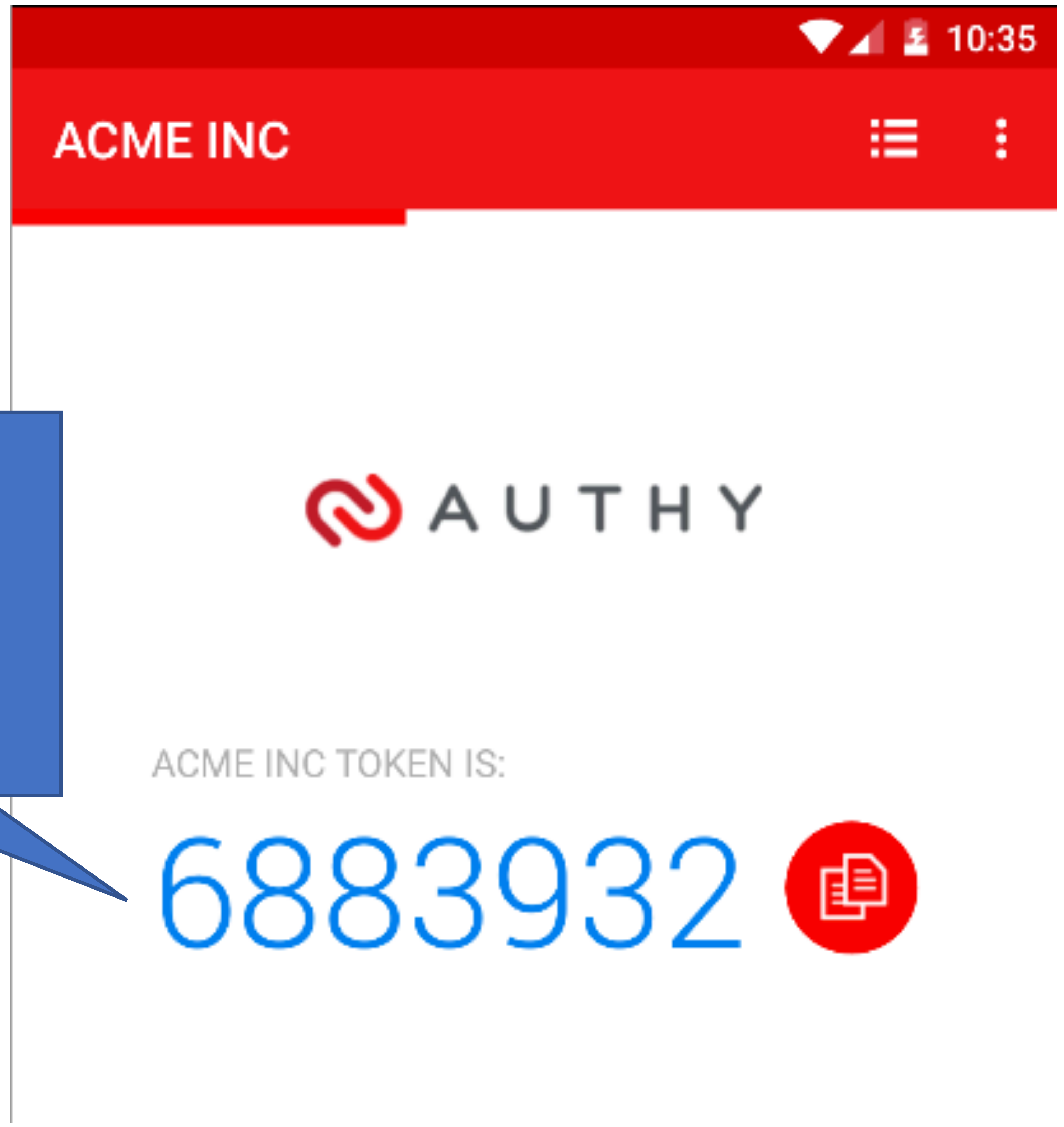
Free T-Mobile Msg: The SIM card for [redacted] has been updated. Account activity details at my.t-mobile.com. Call 1-800-937-8997 if change is unauthorized.

https://www.vice.com/en_us/article/vbqax3/hackers-sim-swapping-steal-phone-numbers-instagram-bitcoin

One Time Passwords

- Generate ephemeral passcodes that change over time
- To login, supply normal password and the current one time password
- Relies on a shared secret between your mobile device and the service provider
  - Shared secret allows both parties to know the current one time password

Changes every few minutes



ACME INC TOKEN IS:

6883932

Duo Mobile

Lastpass Authenticator

Google Authenticator

Time-based One-time Password Algorithm

$T0$ = <the beginning of time, typically Thursday, 1 January 1970 UTC>

TI = <length of time the password should be valid>

K = <shared secret key>

d = <the desired number of digits in the password>

TC = floor((unixtime(now) − unixtime($T0$)) / TI),

TOTP = HMAC(K, TC) % 10^{d}

Specially formatted SHA1-based signature

Time-based One-time Password Algorithm

T0 = <the beginning of time, typically Thursday, 1 January 1970 UTC>

TI = <length of time the password should be valid>

K = <shared secret key>

d = <the desired number of digits in the password>

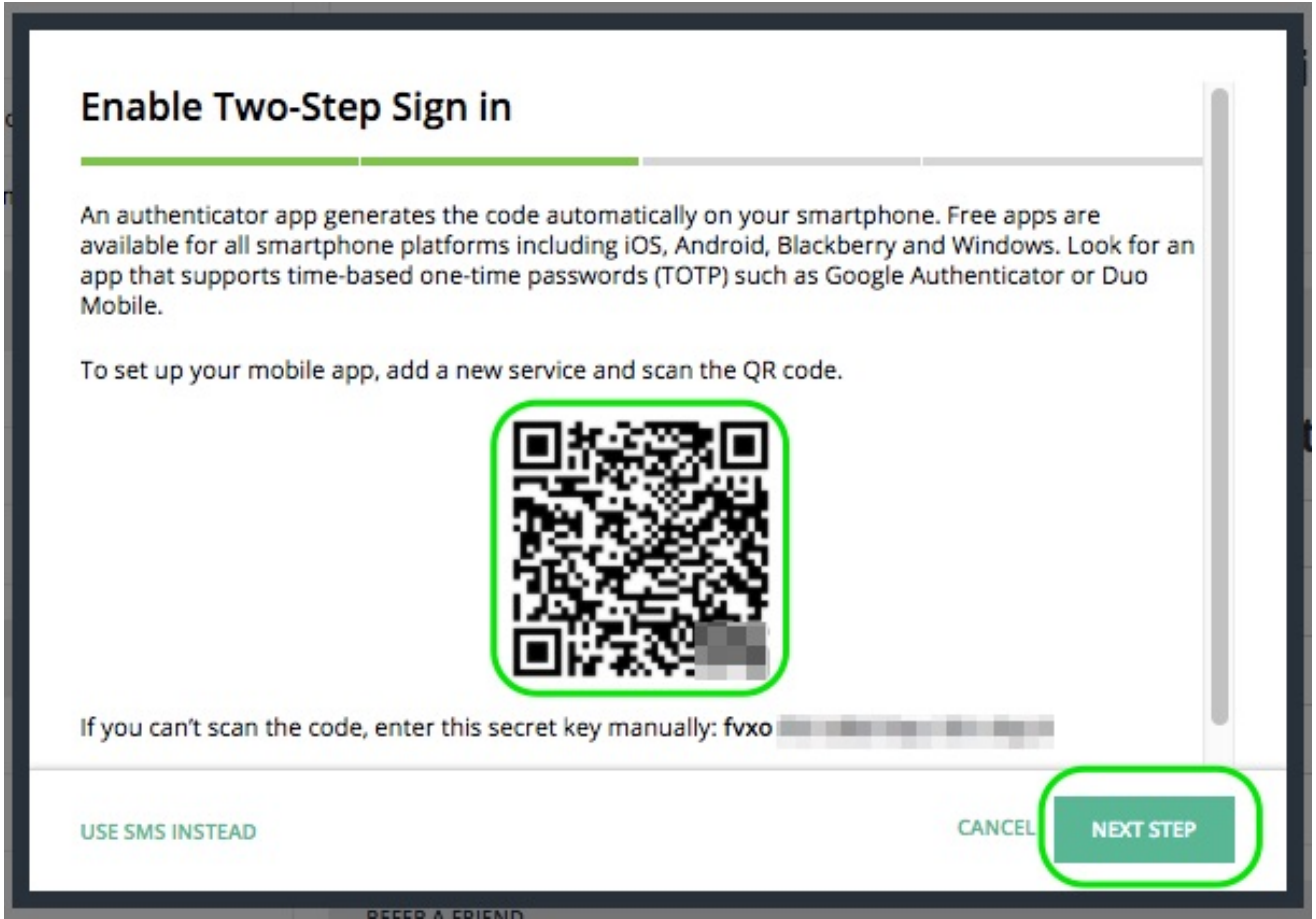
$TC = \text{floor}((\text{unixtime}(\text{now}) - \text{unixtime}(T0)) \mathbin{/} TI),$

$\text{TOTP} = \text{HMAC}(K, TC) \mathbin{\%} 10^{d}$

Specially formatted SHA1-based signature

Given *K*, this algorithm can be run on your phone and by the service provider

Secret Sharing for TOTP



Enable Two-Step Sign in

An authenticator app generates the code automatically on your smartphone. Free apps are available for all smartphone platforms including iOS, Android, Blackberry and Windows. Look for an app that supports time-based one-time passwords (TOTP) such as Google Authenticator or Duo Mobile.

To set up your mobile app, add a new service and scan the QR code.

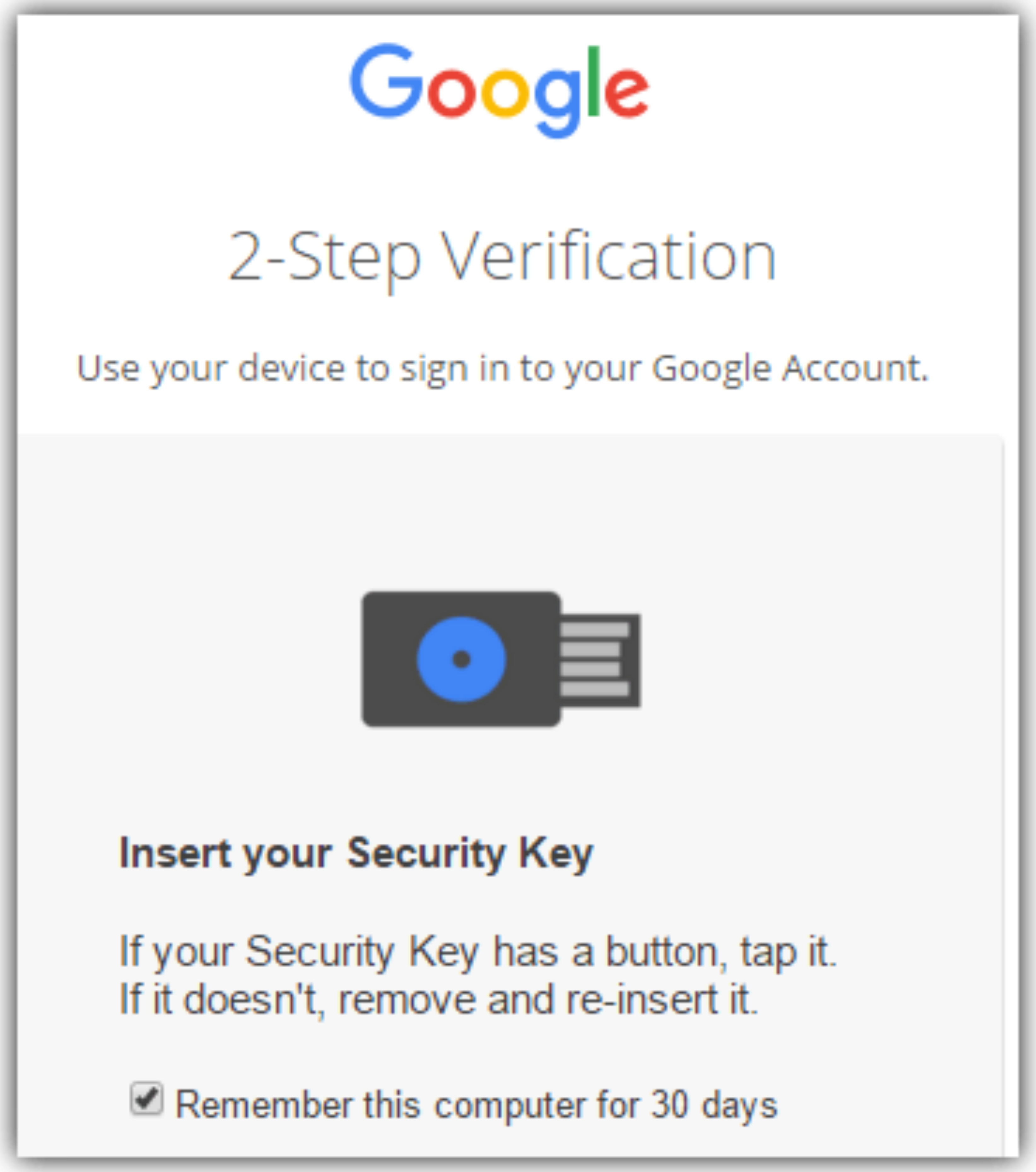
If you can't scan the code, enter this secret key manually: **fvxo** [redacted]

Hardware Two Factor

- Special hardware designed to hold cryptographic keys
- Physically resistant to key extraction attacks
  - E.g. scanning tunneling electron microscopes
- Uses:
  - 2nd factor for OS log-on
  - 2nd factor for some online services
  - Storage of PGP and SSH keys

Universal 2nd Factor (U2F)

- Supported by Chrome, Opera, and Firefox (must be manually enabled)
- Works with Google, Dropbox, Facebook, Github, Gitlab, etc.



Google

2-Step Verification

Use your device to sign in to your Google Account.

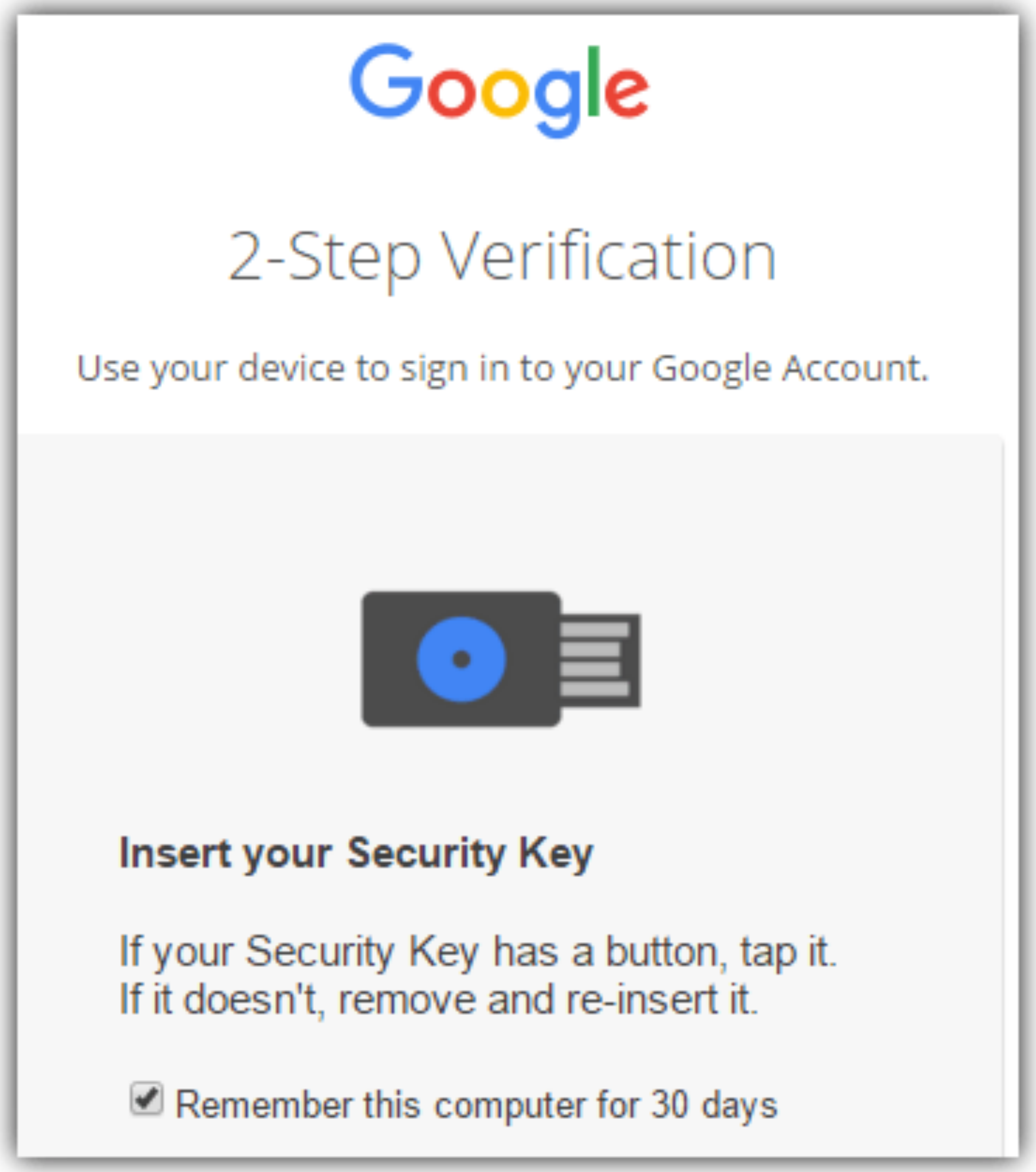
Insert your Security Key

If your Security Key has a button, tap it.
If it doesn't, remove and re-insert it.

☑ Remember this computer for 30 days

Universal 2nd Factor (U2F)

- Supported by Chrome, Opera, and Firefox (must be manually enabled)
- Works with Google, Dropbox, Facebook, Github, Gitlab, etc.
- Pro tip: always buy 2 security keys
  - Associate both with your accounts
  - Keep one locked in a safe, in case you lose your primary key ;)



Google

2-Step Verification

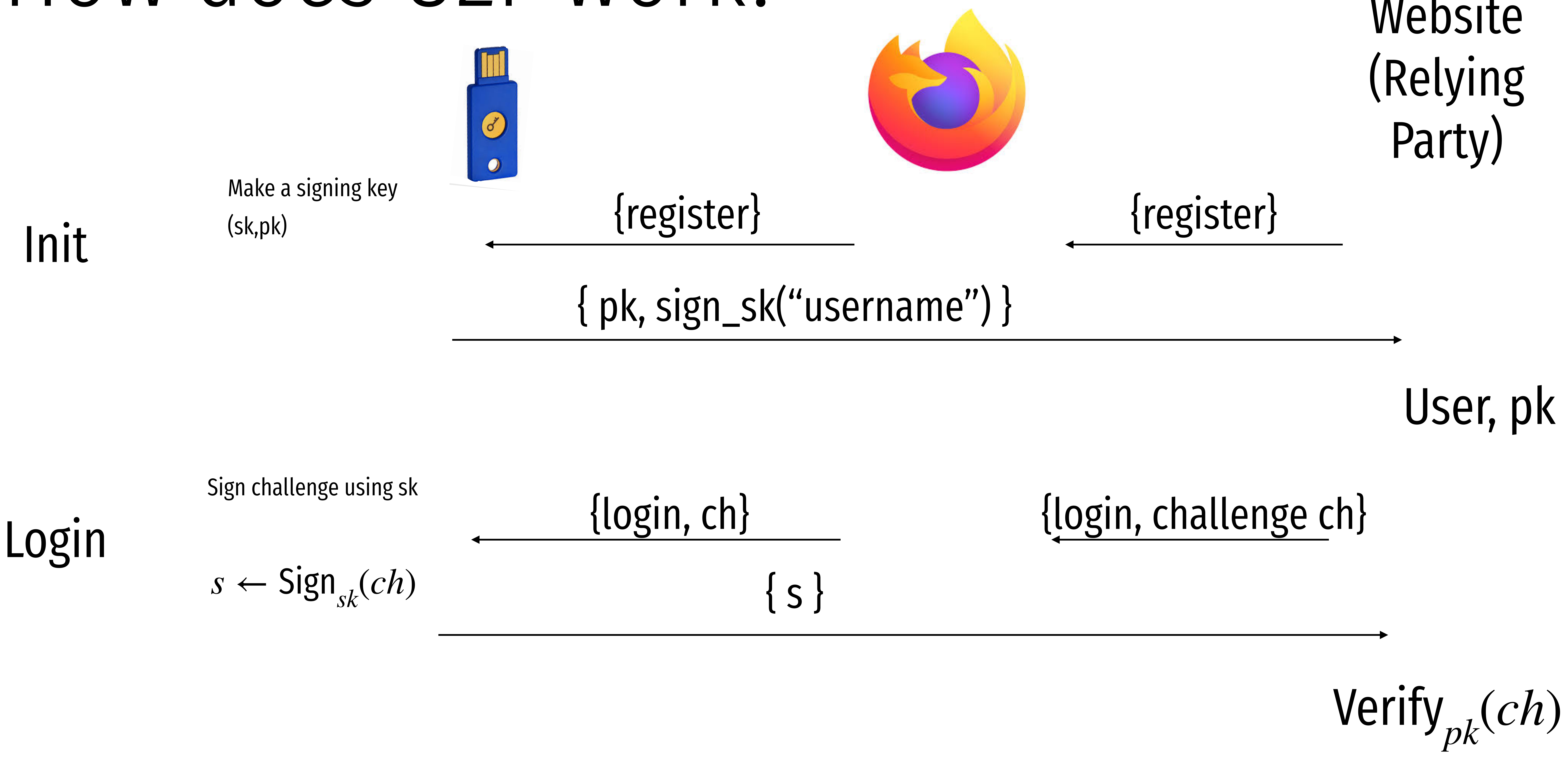
Use your device to sign in to your Google Account.

Insert your Security Key

If your Security Key has a button, tap it.
If it doesn't, remove and re-insert it.

☑ Remember this computer for 30 days

How does U2F work?



Website (Relying Party)

Init

Make a signing key (sk,pk)

{register}

{register}

{ pk, sign_sk(“username”) }

User, pk

Login

Sign challenge using sk

{login, ch}

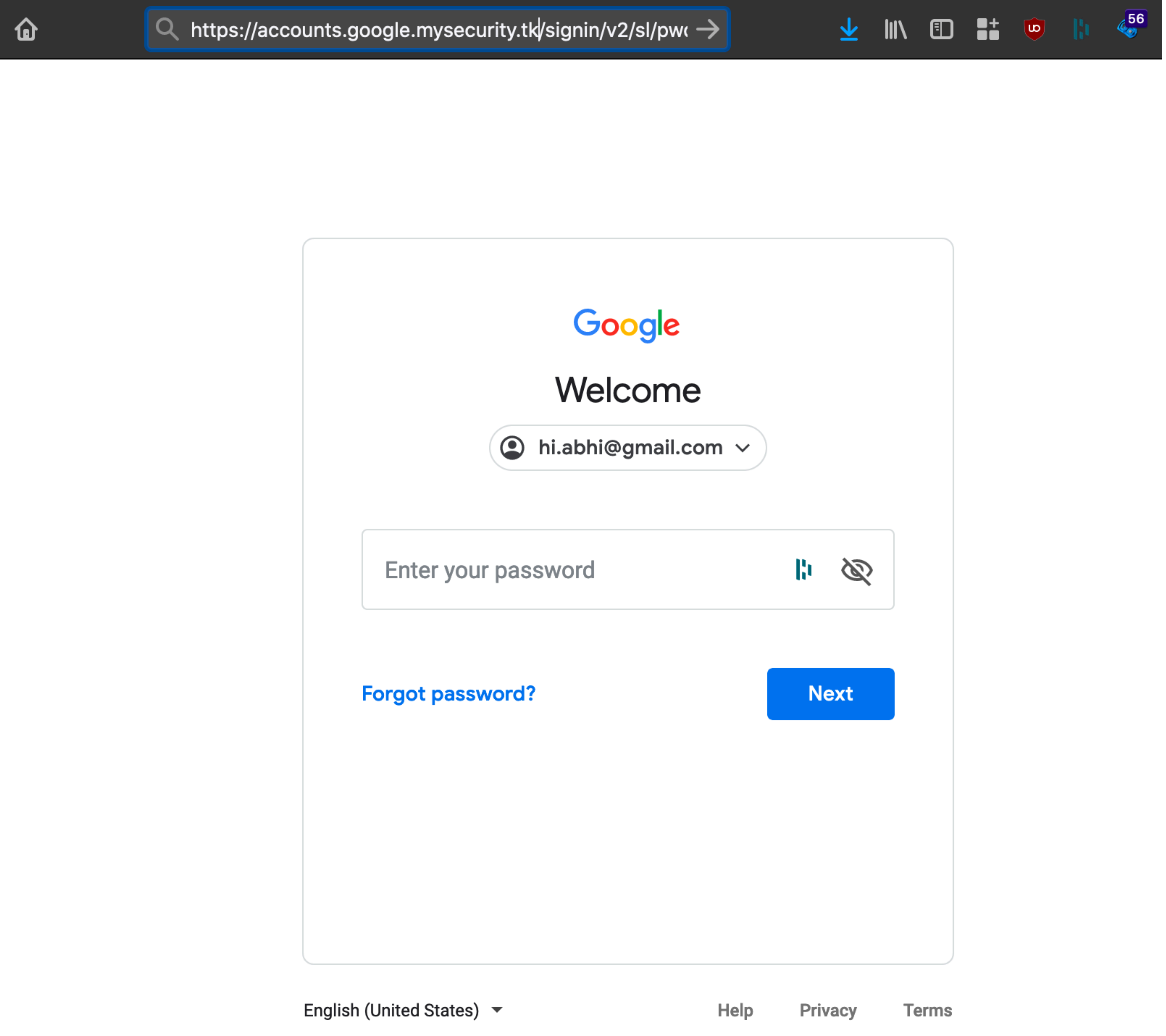
{login, challenge ch}

$s \leftarrow \text{Sign}_{sk}(ch)$

{ s }

$\text{Verify}_{pk}(ch)$

Vulnerable to simple attack



https://accounts.google.mysecurity.tk/signin/v2/sl/pwd

Google

Welcome

hi.abhi@gmail.com

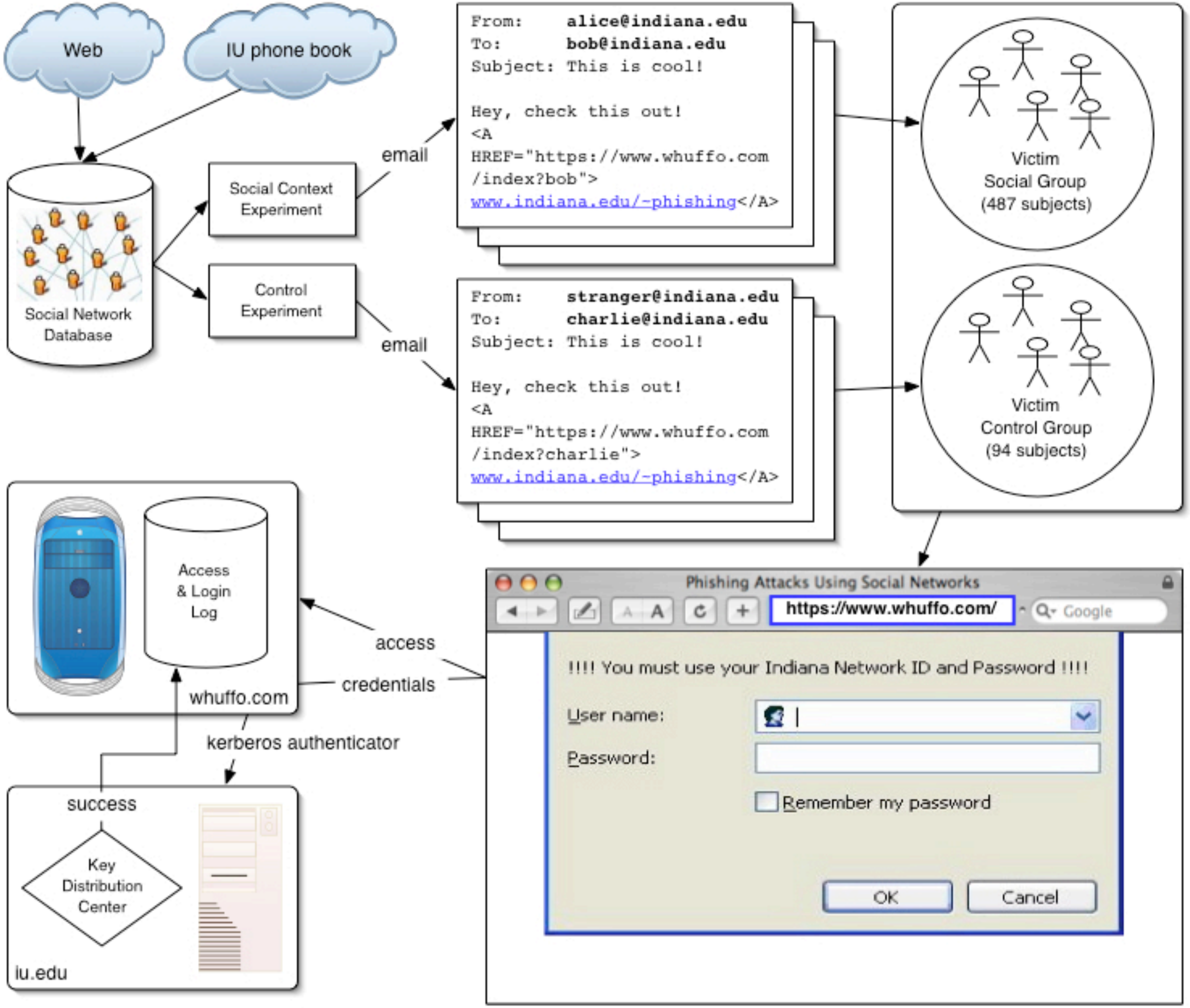
Simple Phishing

Lure: A spammed email with a call to action from a seemingly legitimate source encouraging the user to visit a hook website.

Hook: A website designed to mimic legitimate site and collect confidential information.

Spear Phishing @ IU

Experiment by T. Jagatic, N. Johnson, M. Jakobsson, F. Menczer.



```
From:    alice@indiana.edu
To:      bob@indiana.edu
Subject: This is cool!

Hey, check this out!
<A
HREF="https://www.whuffo.com
/index?bob">
www.indiana.edu/~phishing</A>
```

```
From:    stranger@indiana.edu
To:      charlie@indiana.edu
Subject: This is cool!

Hey, check this out!
<A
HREF="https://www.whuffo.com
/index?charlie">
www.indiana.edu/~phishing</A>
```

!!!! You must use your Indiana Network ID and Password !!!!

User name:

Password:

□ Remember my password

Control Phishing Success Rate:

9-23%

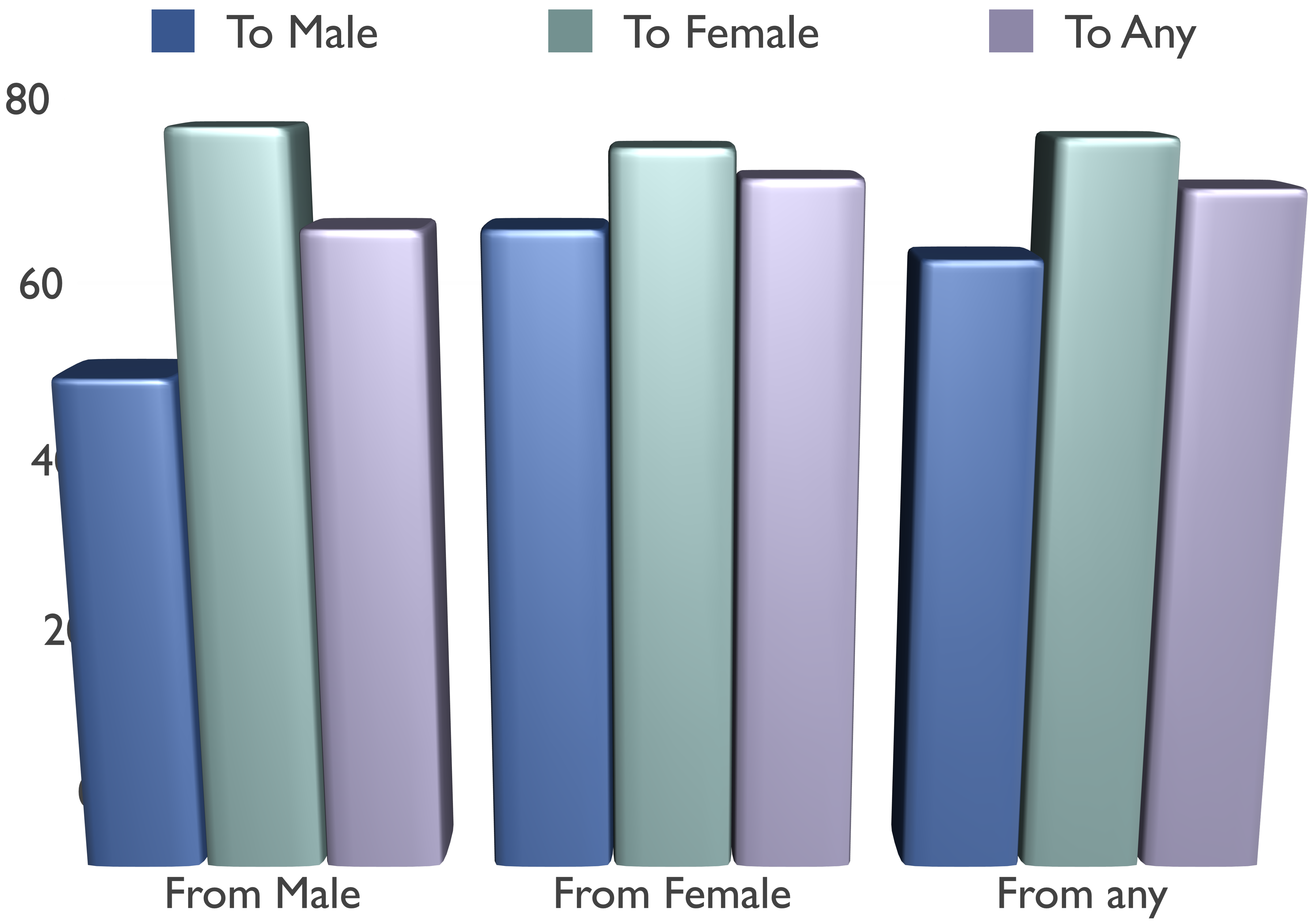
with 95% Confidence Interval

Spear Phishing Success Rate:

68-72%

with 95% Confidence Interval

Spear Phishing Success Rate by Gender



VOIP Phishing

Lure: Get victim to call a bogus 800... number about their account.

Hook: Have the human on the other end extract the victim’s information.

From: FlagStar Bank <usflag60536@flagstar.com>
Date: 11 Sep 2007 10:55:21 -0400
To: <samyers@indiana.edu>
Subject: You have one new private message

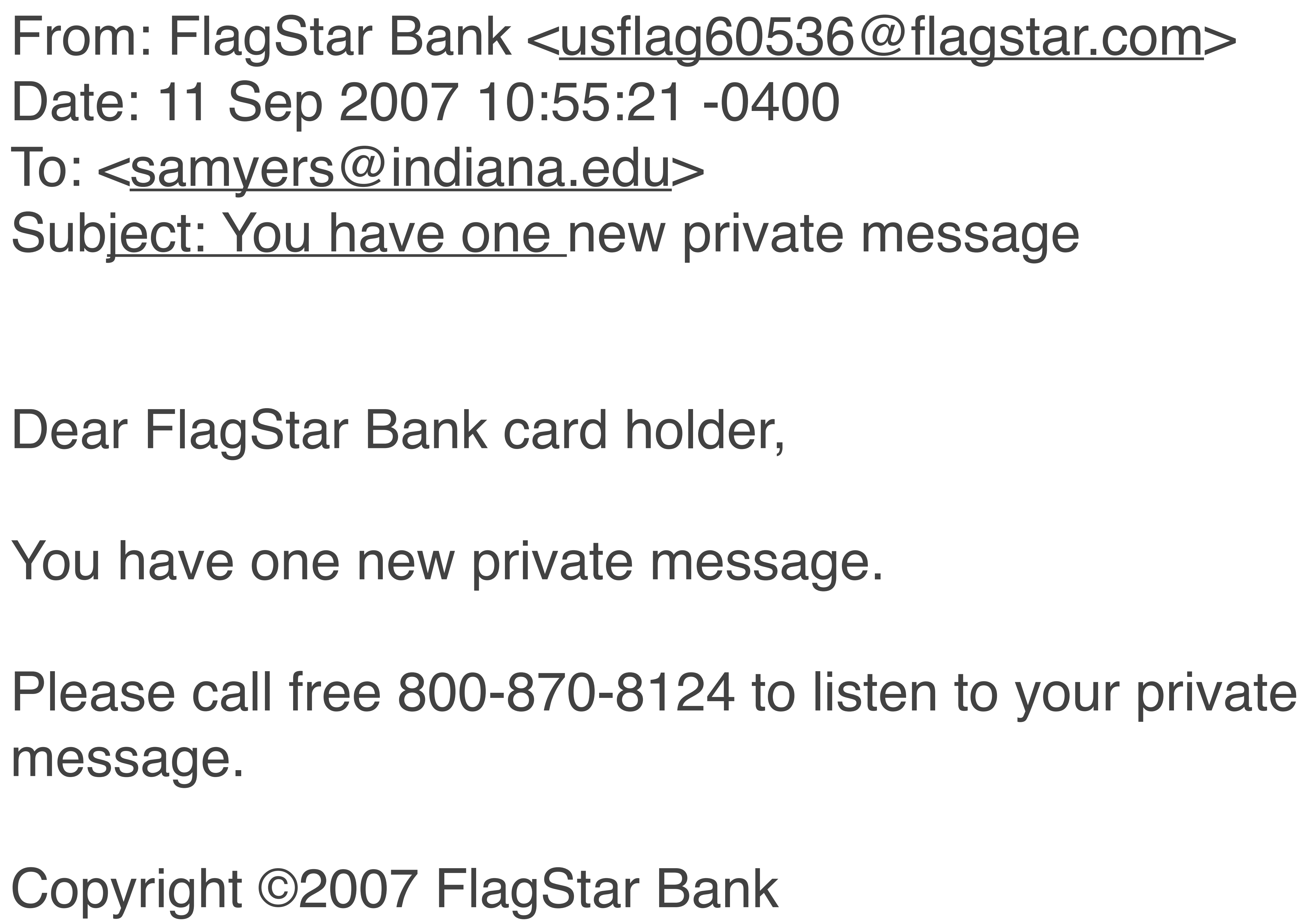
Dear FlagStar Bank card holder,

You have one new private message.

Please call free 800-870-8124 to listen to your private message.

Copyright ©2007 FlagStar Bank

Source: Steven Myers, IU



From: FlagStar Bank <usflag60536@flagstar.com>
Date: 11 Sep 2007 10:55:21 -0400
To: <samyers@indiana.edu>
Subject: You have one new private message

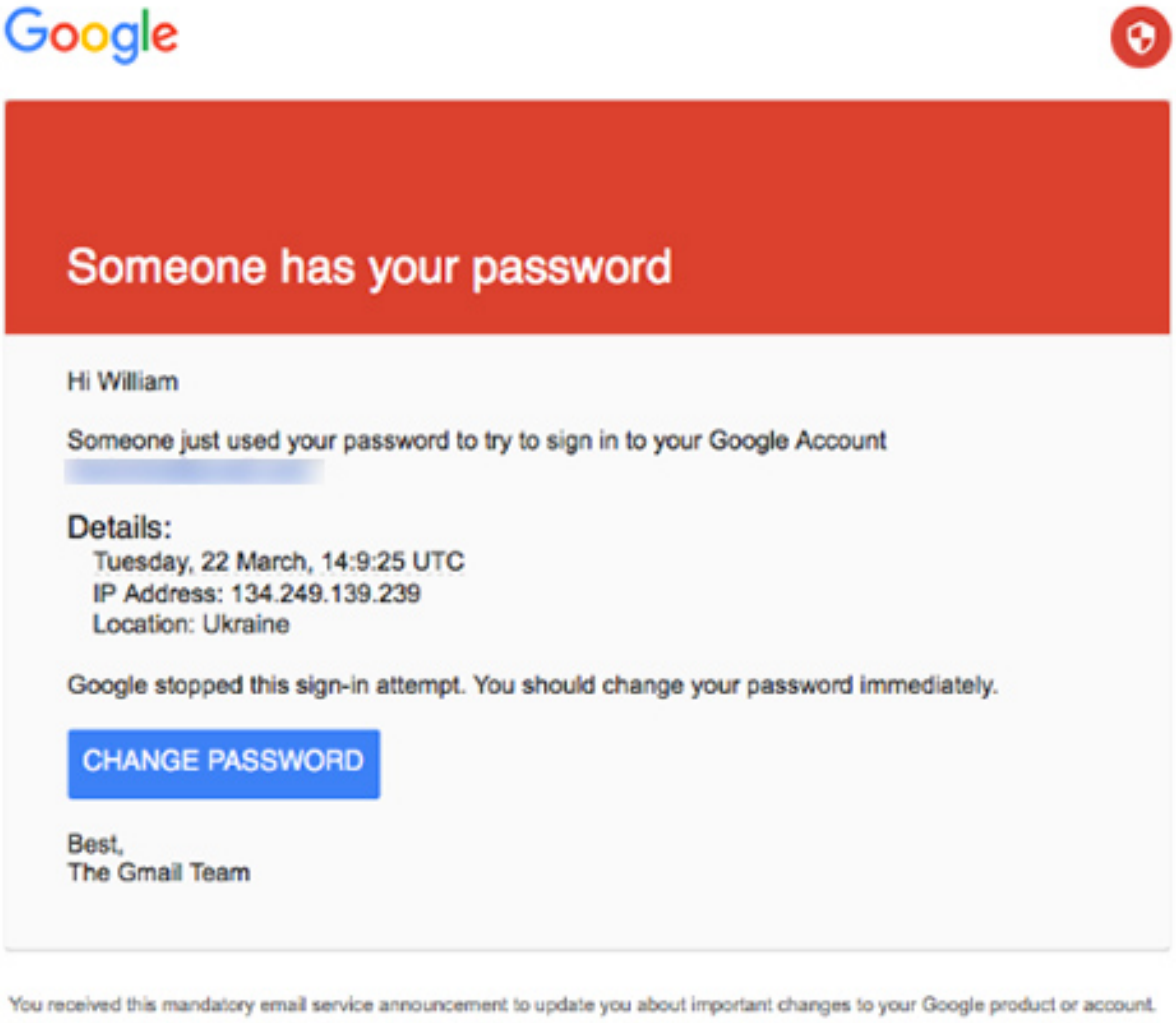
Dear FlagStar Bank card holder,

You have one new private message.

Please call free 800-870-8124 to listen to your private message.

Copyright ©2007 FlagStar Bank

Source: Steven Myers, IU



Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Account
[redacted]

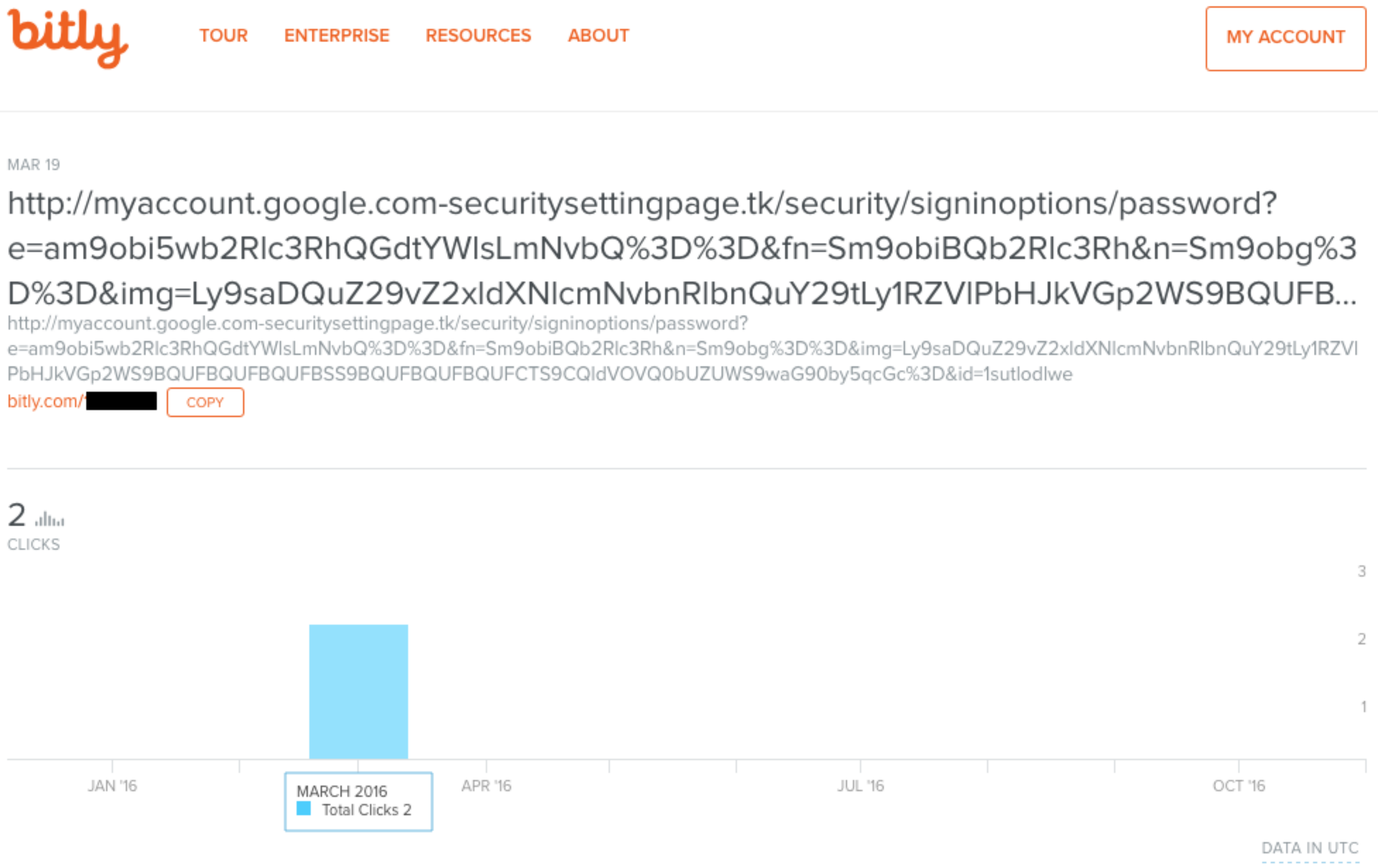
Details:

Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

Best,
The Gmail Team

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



MAR 19

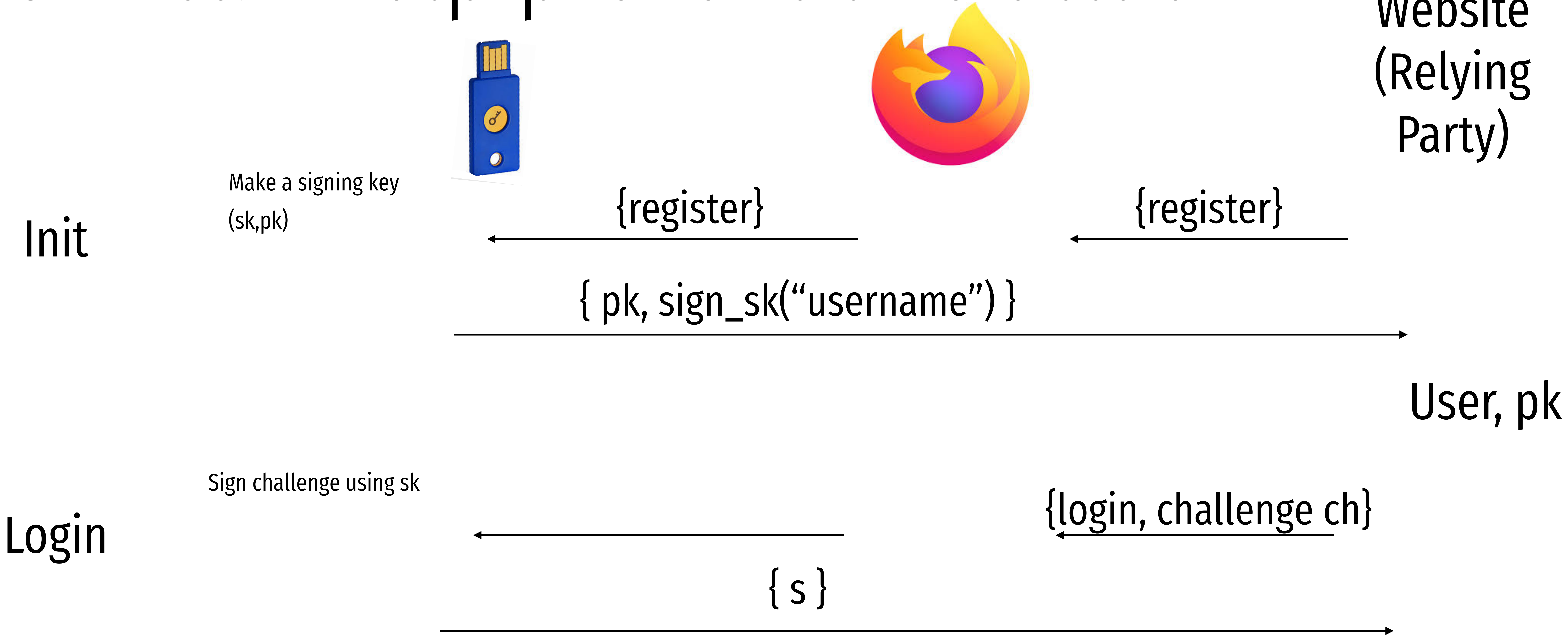
http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFB...

http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFCTS9CQldVOVQ0bUZUWS9waG90by5qcGc%3D&id=1sutlodlwe

bitly.com/[redacted] COPY

2
CLICKS

U2F can help prevent this attack



Website (Relying Party)

Init

Make a signing key

(sk,pk)

{register}

{register}

{ pk, sign_sk(“username”) }

User, pk

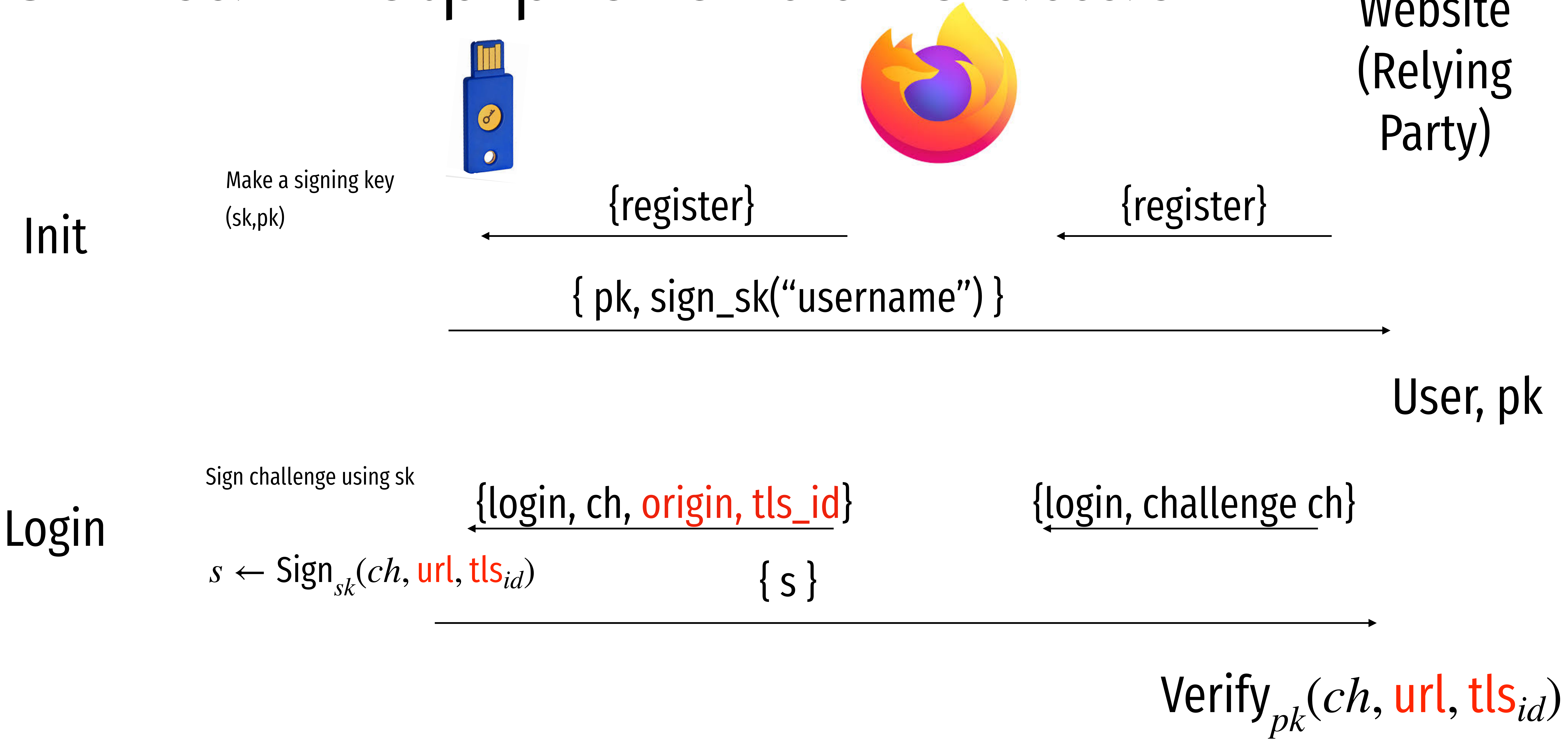
Login

Sign challenge using sk

{login, challenge ch}

{ s }

U2F can help prevent this attack



Website (Relying Party)

Init

Make a signing key (sk,pk)

{register}

{register}

{ pk, sign_sk("username") }

User, pk

Login

Sign challenge using sk

{login, ch, origin, tls_id}

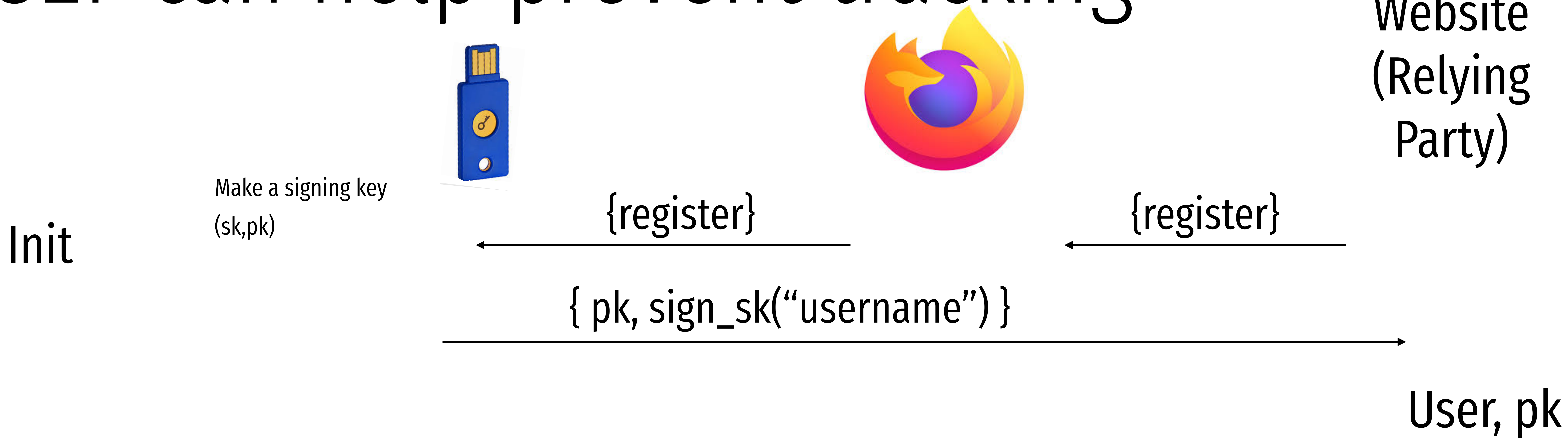
{login, challenge ch}

$s \leftarrow \text{Sign}_{sk}(ch, \text{url}, \text{tls}_{id})$

{ s }

$\text{Verify}_{pk}(ch, \text{url}, \text{tls}_{id})$

U2F can help prevent tracking



Website (Relying Party)

Init

Make a signing key (sk,pk)

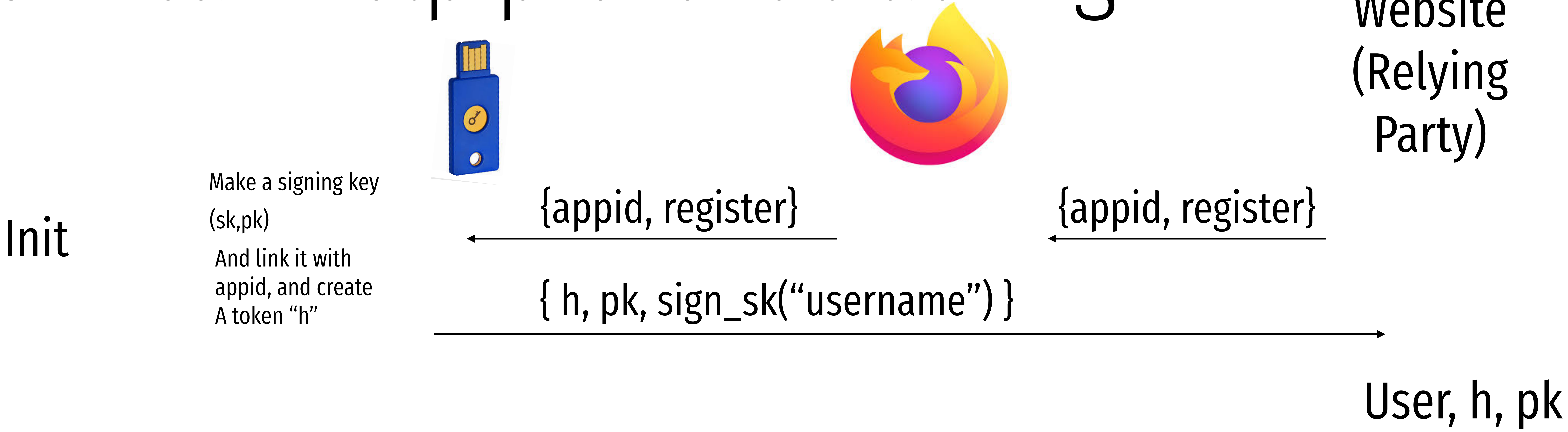
{register}

{register}

{ pk, sign_sk(“username”) }

User, pk

U2F can help prevent tracking



Website (Relying Party)

Init

Make a signing key (sk,pk)

And link it with appid, and create A token “h”

{appid, register}

{appid, register}

{ h, pk, sign_sk(“username”) }

User, h, pk

U2F can help prevent tracking

Website (Relying Party)

Init

Make a signing key

(sk,pk)

And link it with appid, and create A token “h”

{appid, register}

{appid, register}

{ h, pk, sign_sk(“username”) }

User, h, pk

Login

Lookup sk using h
Sign challenge using sk

$s \leftarrow \text{Sign}_{sk}(ch, \text{url}, \text{tls}_{id})$

{login, h, ch, origin, tls_id}

{login, appid, challenge ch}

{ s,h }

$\text{Verify}_{pk}(ch, \text{url}, \text{tls}_{id})$

Check h

```
Sending request with appId: https://u2f.bin.coffee
{
  "version": "U2F_V2",
  "challenge": "uQnl3M4Rj3FZgs6WjyLaZAfwRh4"
}

Got response:
{
  "clientData": "eyJjaGFsbGVuZ2UiOiJ1UW5sM000UmozRlpnczZXanlMYVpBZndSaDQiLCJvcmlnaW4iOiJodHRwczovL3UyZi5iaW4uY29mZmVlIiwidHlwIjoibmF2
  "errorCode": 0,
  "registrationData": “BQRSuRLPv0p5udQ55vVhucf3N50q6…”,
  "version": "U2F_V2"
}

Key Handle: 0r0Z0p0F0E0-0d0W0c0Q0b0X0i020C0w0-0E0v0h0t0T0T0P0_0-090_0a050P0e030u0b0z0l0K0Q0r0O0f0u030_0P020B0J0M0x0D050J0_0d0P0Q0e0j0
Certificate: 3082021c3082…
Attestation Cert
Subject: Yubico U2F EE Serial 14803321578
Issuer: Yubico U2F Root CA Serial 457200631
Validity (in millis): 1136332800000
Attestation Signature
R: 00b11e3efe5ae5ac7ca0e0d4fe2c5b5cf18a2531c0f4f70b11c30b72b5f946a9a3
S: 0f37ab2d4f93ebcdaed0a51b4b17fb93403db9873f0e9cce36f17b1502734bb2
[PASS] Signature buffer has no unnecessary bytes.: 71 == 71
[PASS] navigator.id.finishEnrollment == navigator.id.finishEnrollment
[PASS] uQnl3M4Rj3FZgs6WjyLaZAfwRh4 == uQnl3M4Rj3FZgs6WjyLaZAfwRh4
[PASS] https://u2f.bin.coffee == https://u2f.bin.coffee
[PASS] Verified certificate attestation signature
[PASS] Imported credential public key
Failures: 0 TODOs: 0
```

Future without passwords?

Authentication Protocols

Unix, PAM, and crypt

Network Information Service (NIS, aka Yellow Pages)

Needham-Schroeder and Kerberos

Status Check

- At this point, we have discussed:
  - How to securely store passwords
  - Techniques used by attackers to crack passwords
  - Biometrics and 2nd factors

Status Check

- At this point, we have discussed:
  - How to securely store passwords
  - Techniques used by attackers to crack passwords
  - Biometrics and 2nd factors
- Next topic: building authentication systems
  - Given a user and password, how does the system authenticate the user?
  - How can we perform efficient, secure authentication in a distributed system?

Building authentication systems

Example PAM Configuration

```
# cat /etc/pam.d/system-auth
#%PAM-1.0

auth required pam_unix.so try_first_pa
auth optional pam_permit.so
auth required pam_env.so

account required pam_unix.so
account optional pam_permit.so
account required pam_time.so

password required pam_unix.so try_first_pass nullok sha512 shadow
password optional pam_permit.so

session required pam_limits.so
session required pam_unix.so
session optional pam_permit.so
```

- Use SHA512 as the hash function
- Use /etc/shadow for storage

Unix Passwords

- Traditional method: *crypt*
  - 25 iterations of DES on a zeroed vector
  - First eight bytes of password used as key (additional bytes are ignored)
  - 12-bit salt
- Modern version of *crypt* are more extensible
  - Support for additional hash functions like MD5, SHA256, and SHA512
  - Key lengthening: defaults to 5000 iterations, up to $10^8 - 1$
  - Full password used
  - Up to 16 bytes of salt

Password Files

- Password hashes used to be in */etc/passwd*
  - World readable, contained usernames, password hashes, config information
  - Many programs read config info from the file…
  - But very few (only one?) need the password hashes

Password Files

- Password hashes used to be in */etc/passwd*
  - World readable, contained usernames, password hashes, config information
  - Many programs read config info from the file…
  - But very few (only one?) need the password hashes
- Turns out, world-readable hashes are **Bad Idea**
- Hashes now located in */etc/shadow*
  - Also includes account metadata like expiration
  - Only visible to root

Password Storage on Linux

/etc/passwd

username:x:UID:GID:full_name:home_directory:shell

```
cbw:x:1001:1000:Christo Wilson:/home/cbw/:/bin/bash
amislove:1002:2000:Alan Mislove:/home/amislove/:/bin/sh
```

/etc/shadow

username:password:last:may:must:warn:expire:disable:reserved

```
cbw:$1$0nSd5ewF$0df/3G7iSV49nsbAa/5gSg:9479:0:10000::::
amislove:$1$l3RxU5F1$:8172:0:10000::::
```

Password Storage on Linux

/etc/passwd

username:x:UID:GID:full_name:home_directory:shell

```
cbw:x:1001:1000:Christo Wilson:/home/cbw/:/bin/bash
n Mislove:/home/amislove/:/bin/sh
```

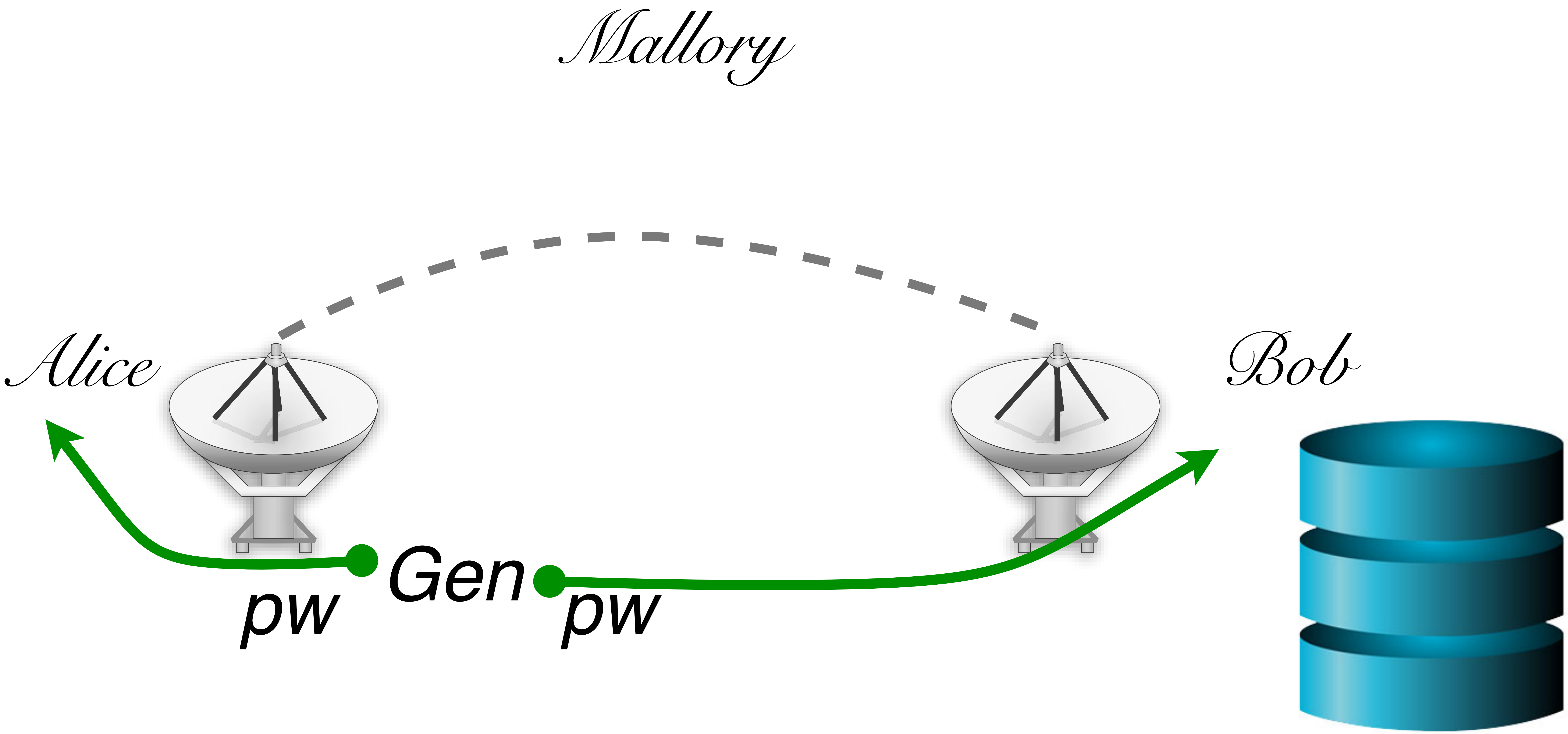
$<algo>$<salt>$<hash>
Algo: 1 = MD5, 5 = SHA256, 6 = SHA512

/etc/shadow

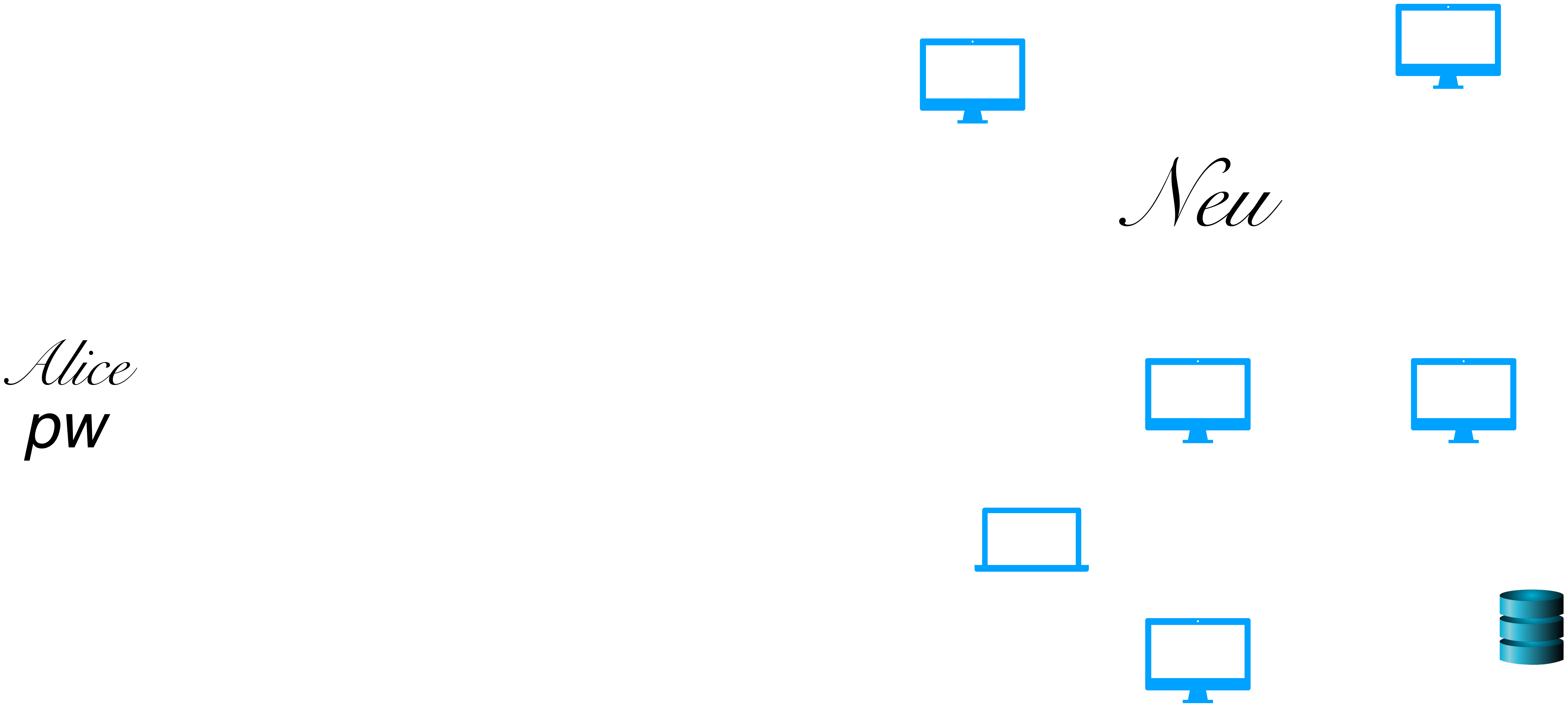
ername:password:last:may:must:warn:expire:disable:reserved

```
cbw:$1$0nSd5ewF$0df/3G7iSV49nsbAa/5gSg:9479:0:10000::::
amislove:$1$l3RxU5F1$:8172:0:10000::::
```

Password Security game



More realistic picture of the world



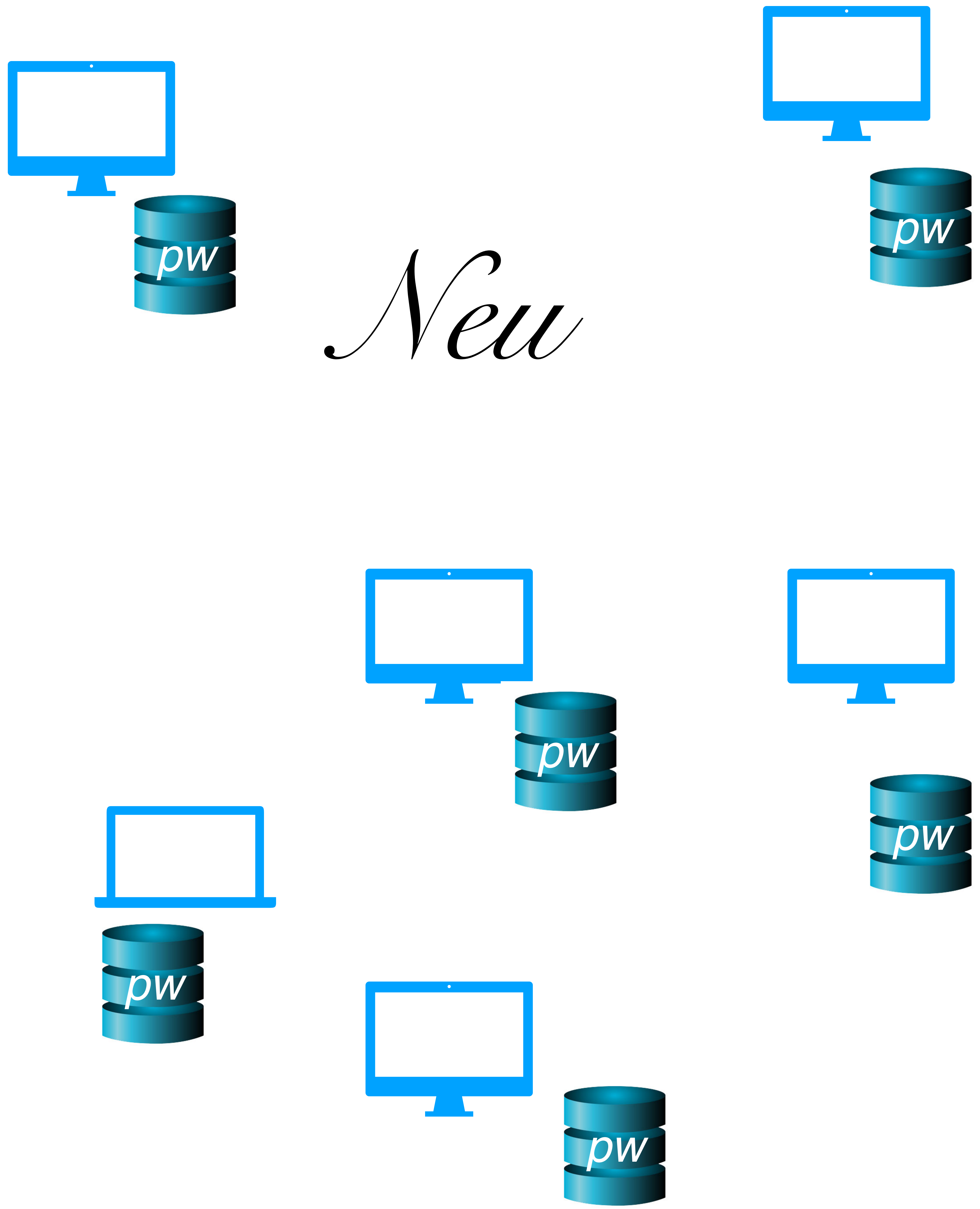
Neu

Alice

pw

More realistic picture of the world

What are the problems with this solution?



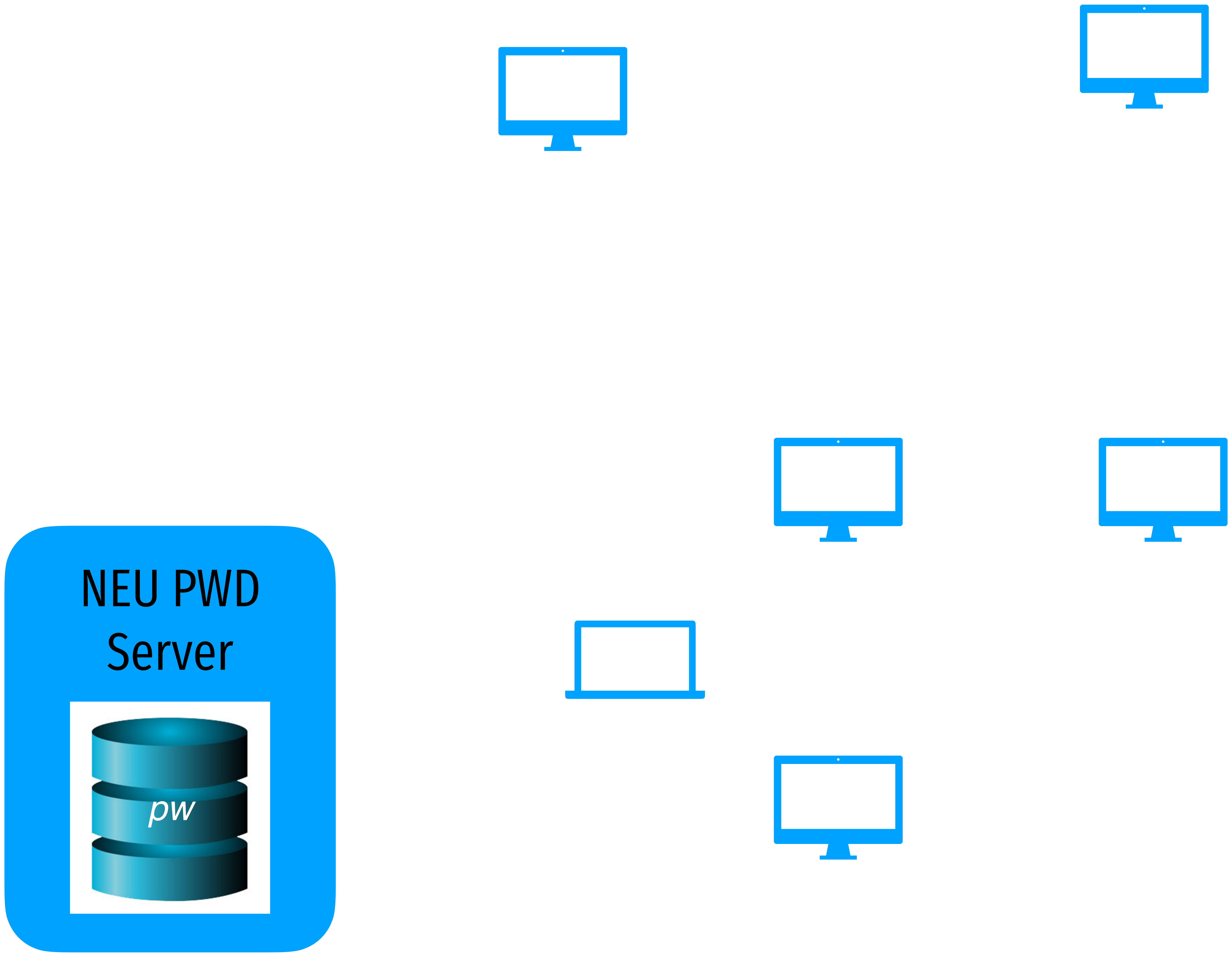
Alice

pw

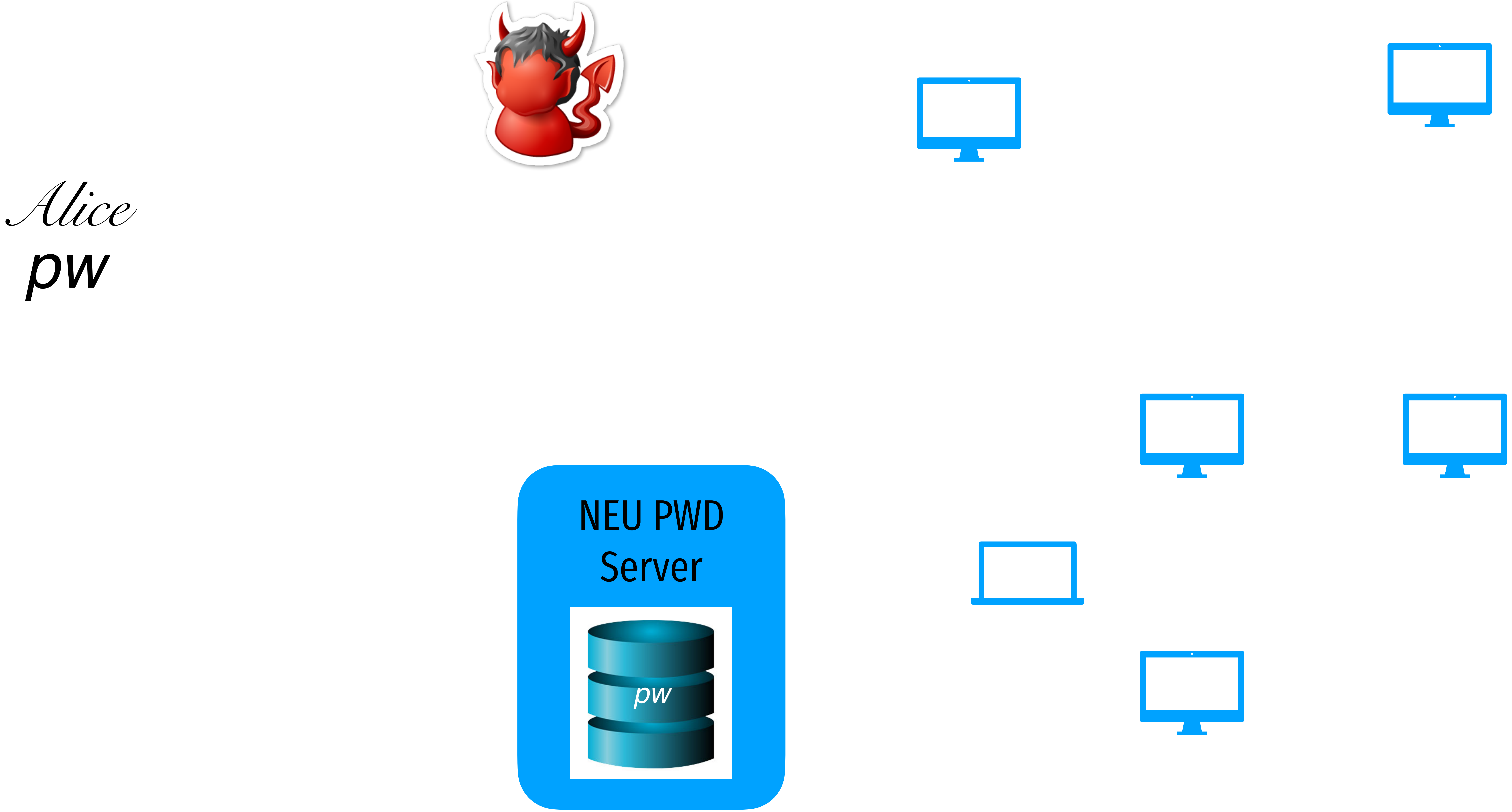
The problem of distributed authentication

Alice

pw



Distributed authentication: Attacker model



What can attacker do?

Alice

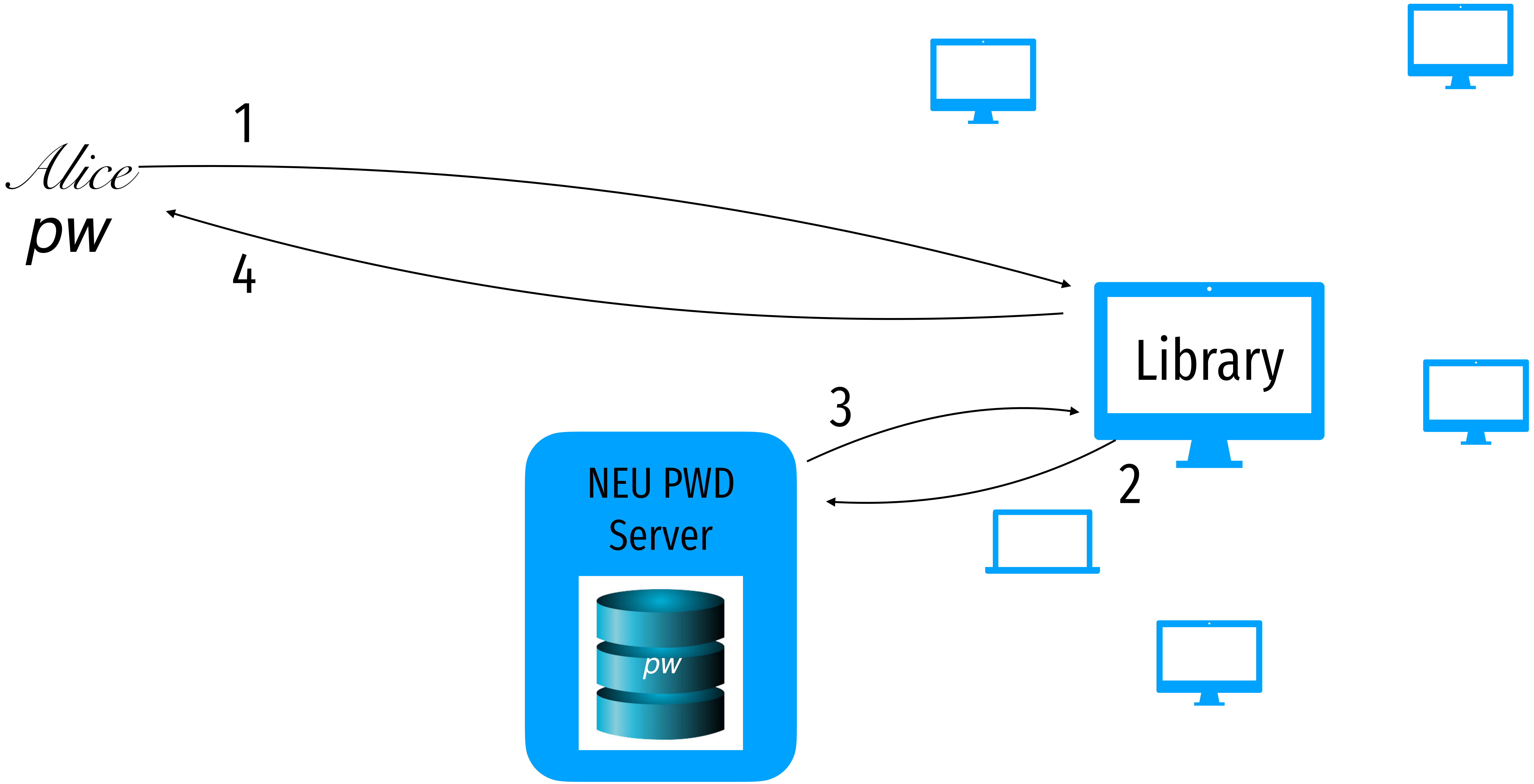
pw

NEU PWD Server

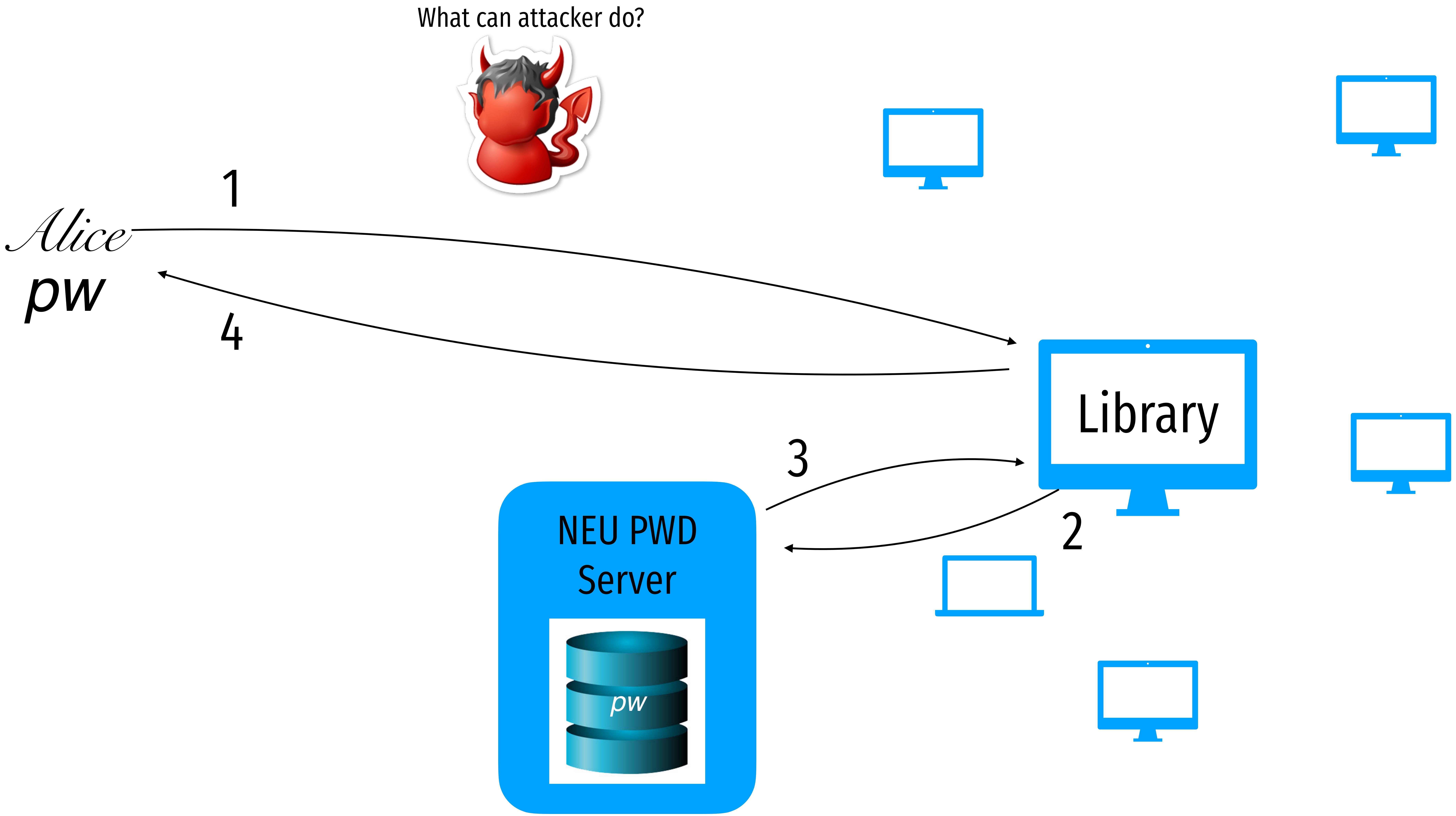
pw

Distributed authentication: Bad Solution

What can attacker do?



Distributed authentication: Bad Solution


What can attacker do?
1
Alice
pw
4
Library
3
2
NEU PWD
Server
pw