twilio

2FA in 2020
…and Beyond!

@kelleyrobinson


@kelleyrobinson

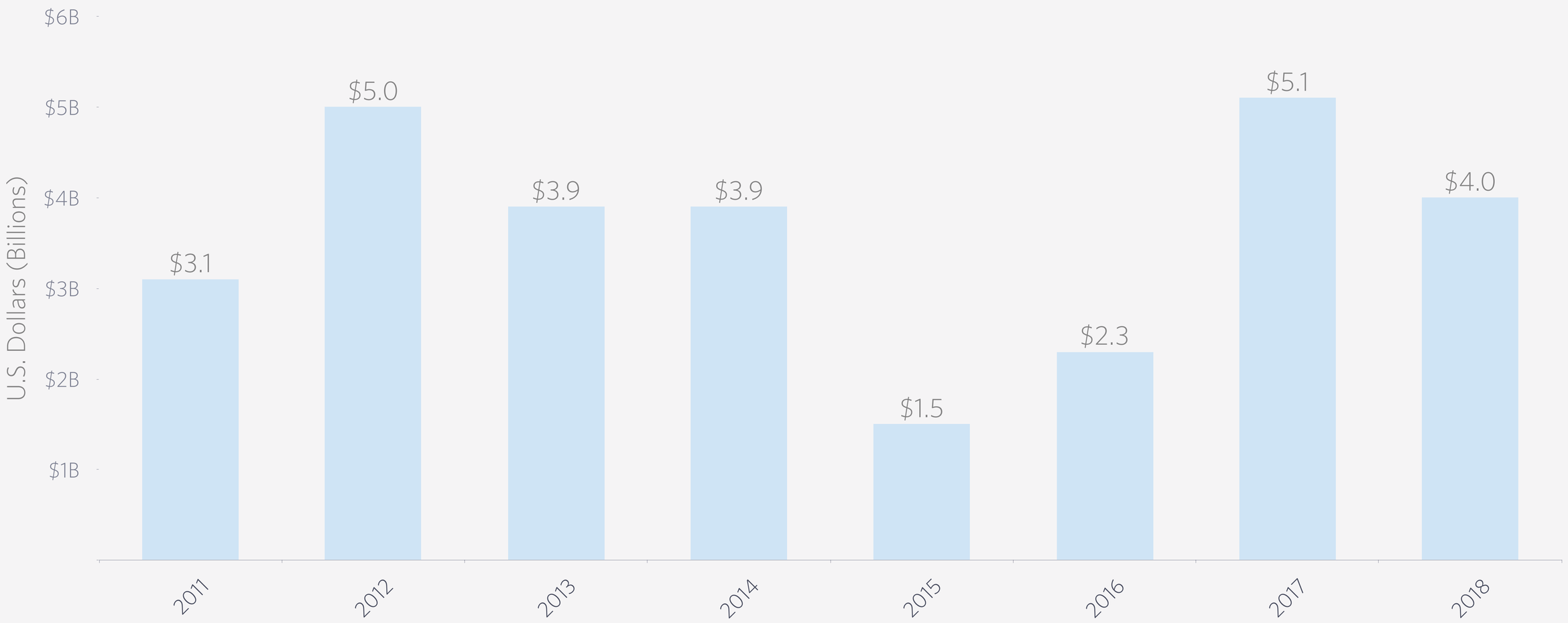

@kelleyrobinson

twilio

@kelleyrobinson

TWILIO
Authy

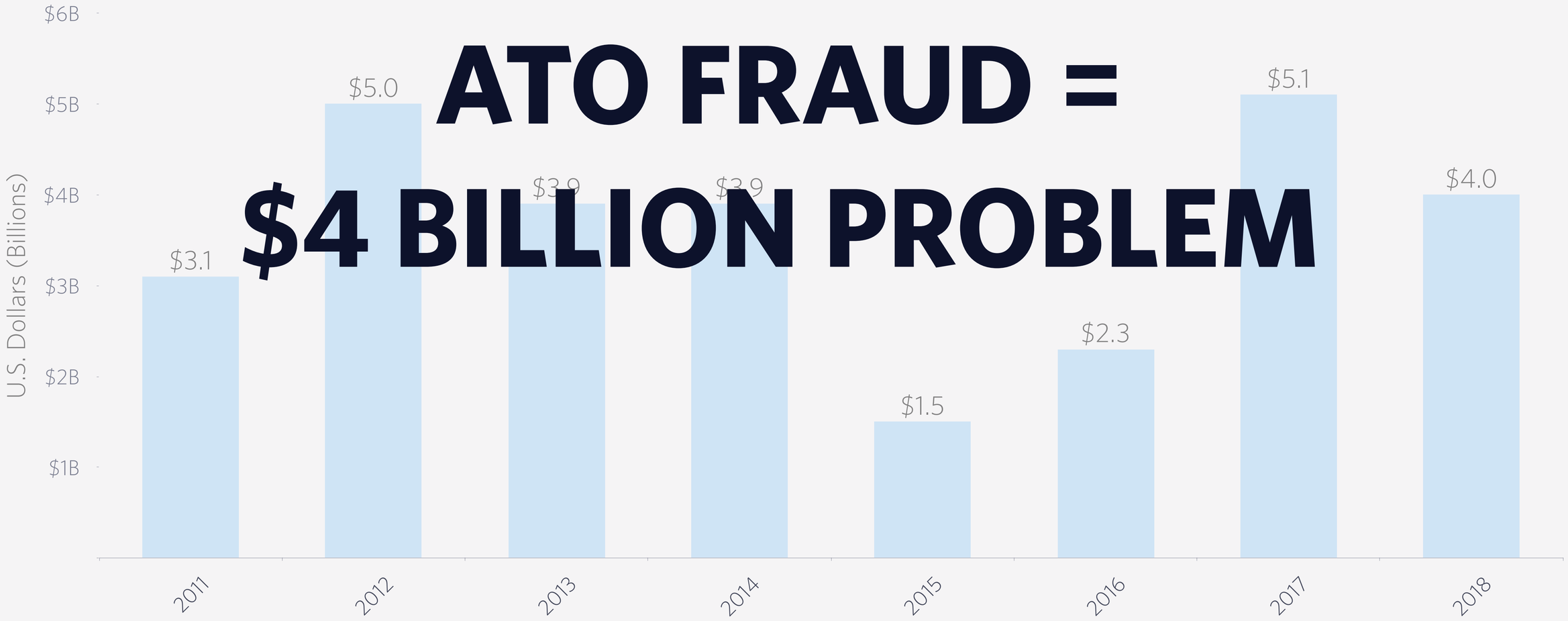
COST OF ACCOUNT TAKEOVER (ATO)



Source: Javelin Strategy & Research, 2019

COST OF ACCOUNT TAKEOVER (ATO)

ATO FRAUD = $4 BILLION PROBLEM



Source: Javelin Strategy & Research, 2019


My
password
123456
End

haveibeenpwned.com

Pwned Passwords

Pwned Passwords are 517,238,891 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online system. Read more about how HIBP protects the privacy of searched passwords.

123456 pwned?

Oh no — pwned!

This password has been seen 22,390,492 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

AUTHENTICATION FACTORS

KNOWLEDGE

i.e. password

POSSESSION

i.e. mobile phone

INHERENCE

i.e. face ID

AUTHENTICATION FACTORS

KNOWLEDGE

i.e. password

POSSESSION

i.e. mobile phone

INHERENCE

i.e. face ID

2FA CHANNELS

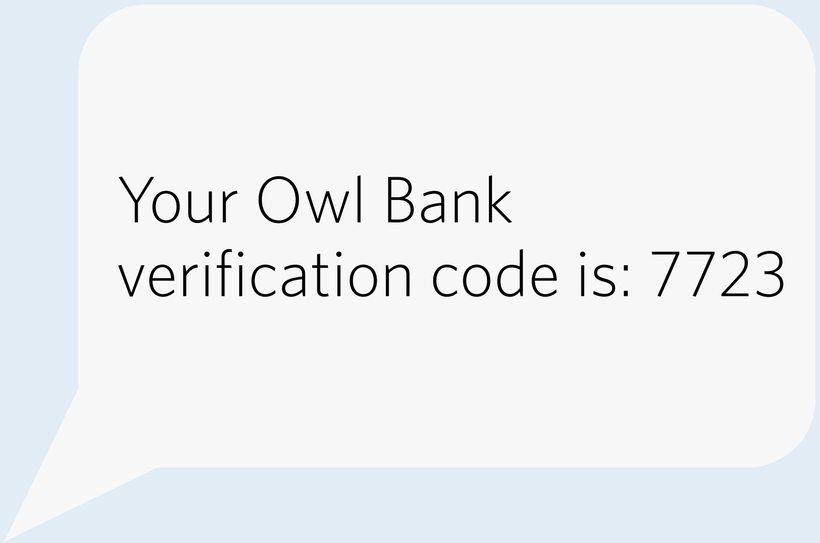
SMS One-time Passwords

✅ Easiest user onboarding

✅ Familiar

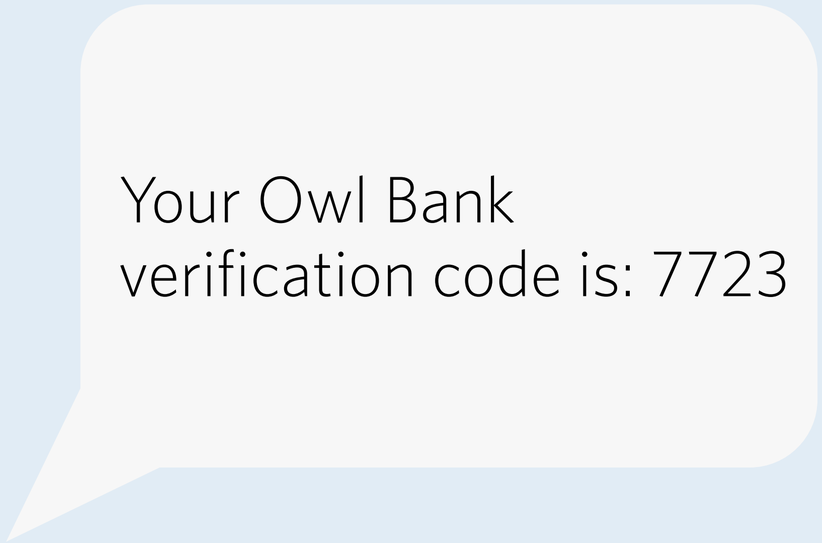
❌ SS7 attacks

❌ SIM swapping



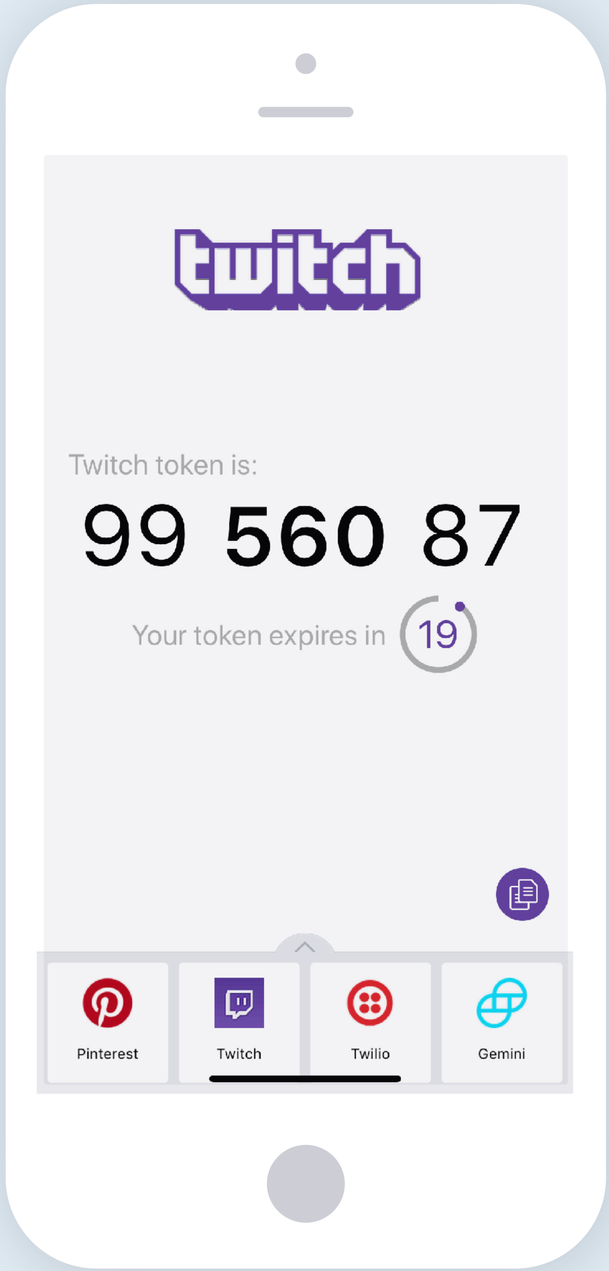
SMS One-time Passwords

Convenient but insecure



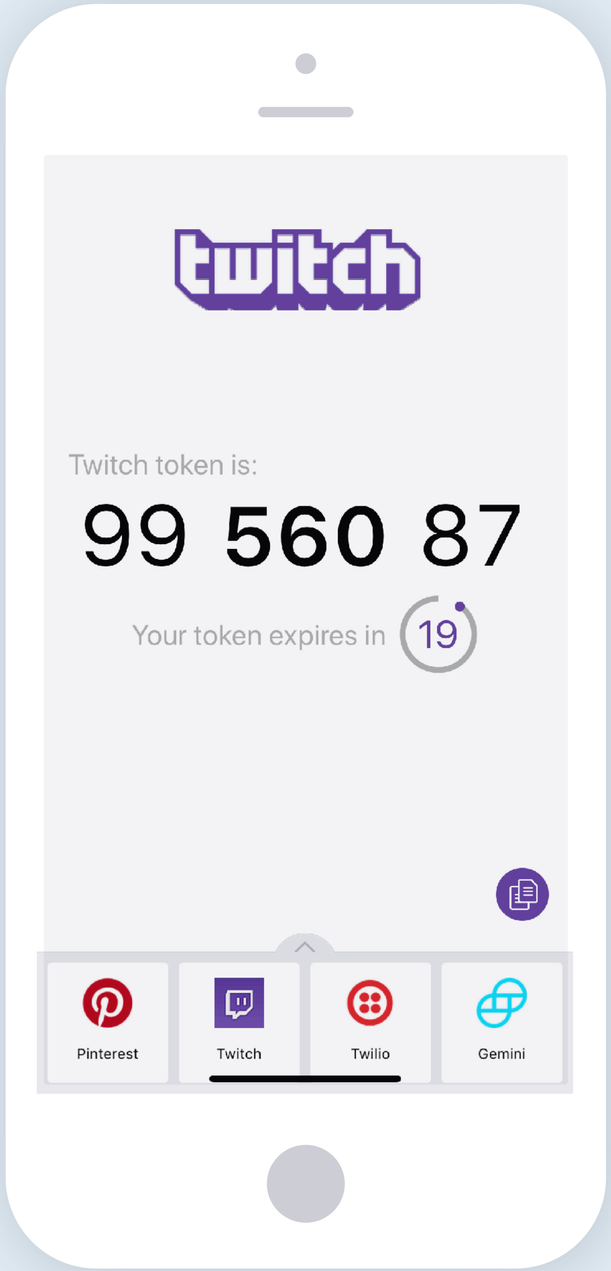
TOTP

- 🔶 Symmetric key crypto
- ✅ Available offline
- ✅ Open standard
- ❌ App install required
- ❌ Expiration UX



TOTP

Pretty good option but not perfect



Push Authentication

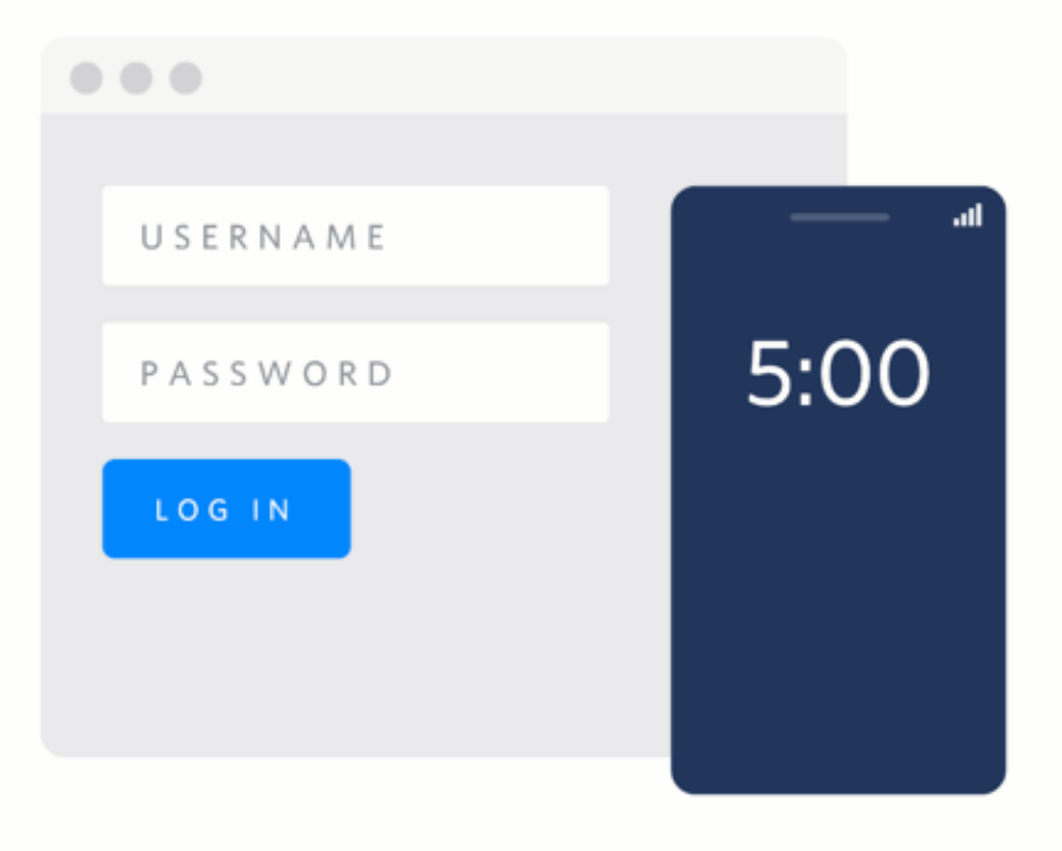
✅ Action context

✅ Denial feedback

✅ Asymmetric key crypto

✅❌ Low friction

🔶 Proprietary



Push Authentication

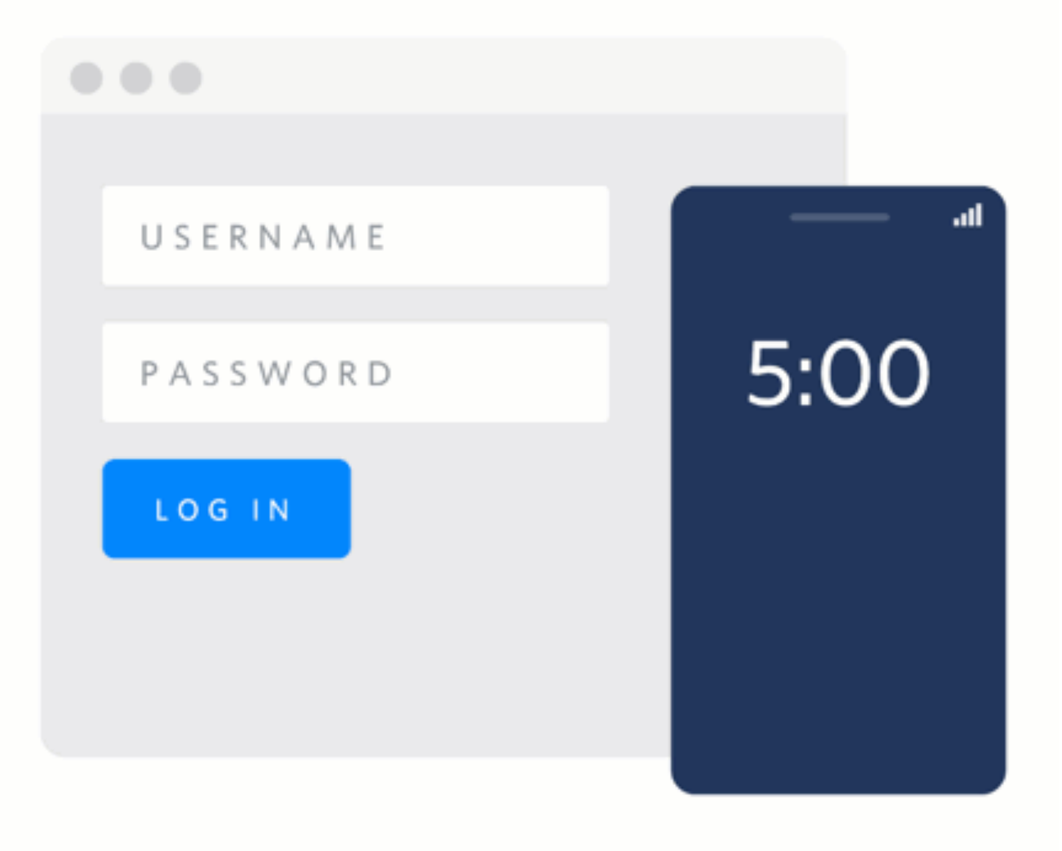
✅ Action context

✅ Denial feedback

✅ Asymmetric key crypto

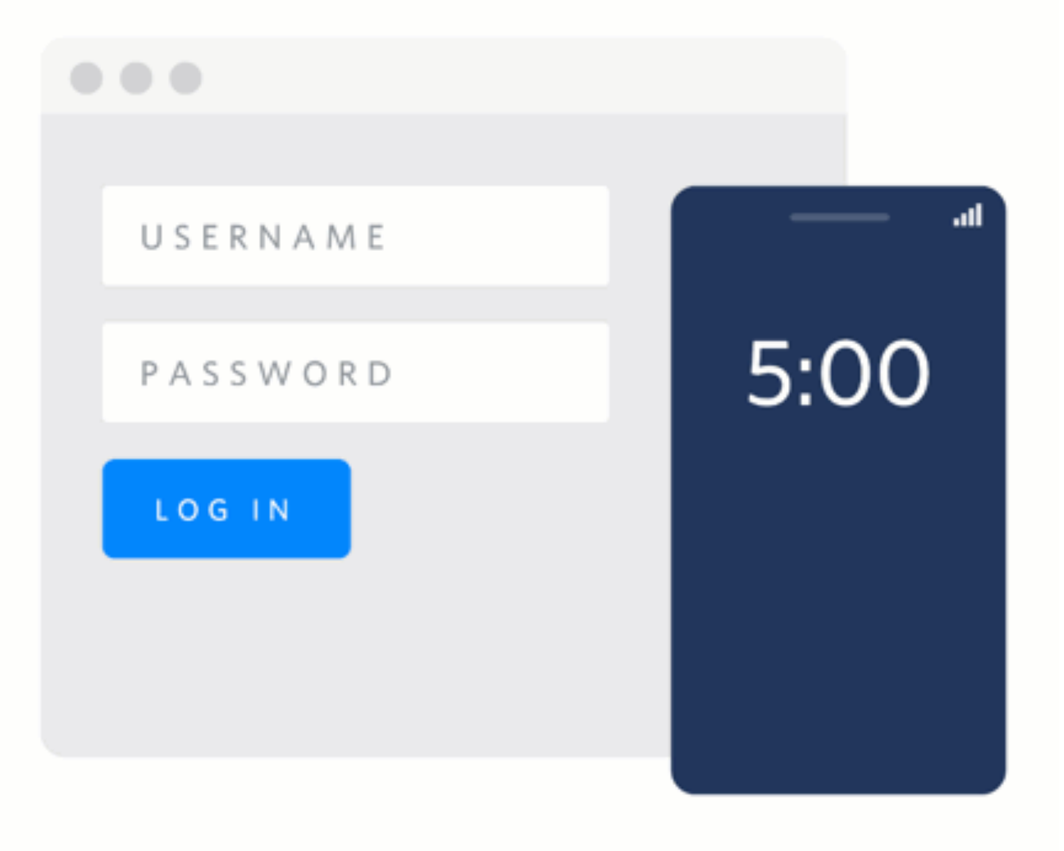
✅❌ Low friction

🔶 Proprietary



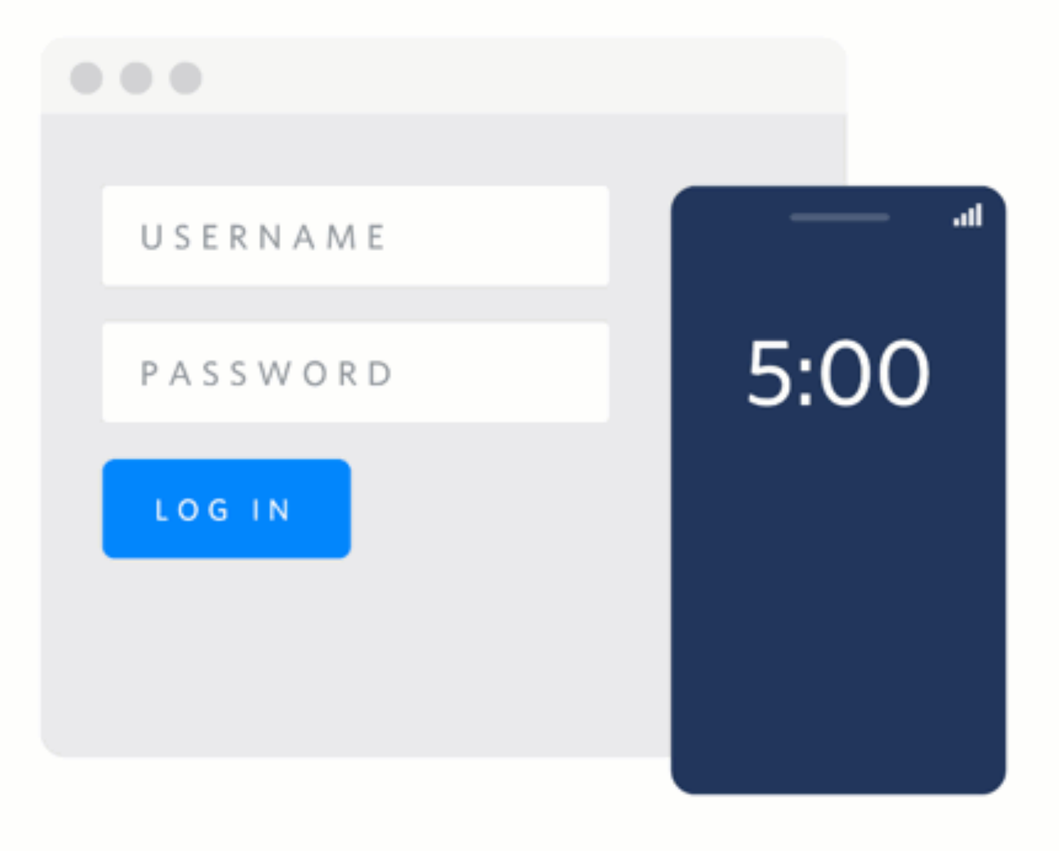
Push Authentication

Convenient and
cryptographically secure,
but maybe too convenient?



Push Authentication

Convenient and
cryptographically secure,
but maybe too convenient?



U2F / WebAuthn

✅ Phishing resistant

✅ Asymmetric key crypto

✅ Open standard

❌ Distribution & cost

❌ New technology

U2F / WebAuthn

Secure but not always convenient. Will become more common.

FACTOR USABILITY

A Usability Study of Five Two-Factor Authentication Methods (BYU 2019)

A Tale of Two Studies: The Best and Worst of YubiKey Usability (UIUC 2018)

State of the Auth Report (Duo Security 2019)

FACTOR SETUP (CROSS-PLATFORM)

😬 YubiKey

Setup success varied a lot based on platform

More people locked themselves out of their computer than successfully set up YubiKey for Windows Logon Authorization Tool

74% requested better documentation

https://isrl.byu.edu/pubs/sp2018.pdf

	N=31	%
Google		
Success	**26**	**83%**
Correctly identified completion	22	70%
Failure	**5**	**16%**
Facebook		
Success	**10**	**32%**
Correctly identified completion	6	19%
Failure	**21**	**67%**
Registered YubiKey without enabling 2FA	12	38%
Windows 10		
Success	**12**	**38%**
Set up the *Windows Logon Authorization Tool*	5	16%
Set up *YubiKey for Windows Hello*	7	22%
Failure	**19**	**61%**
Failed to set up the *Windows Logon Authorization Tool*	9	29%
Failed to set up *YubiKey for Windows Hello*	5	16%
Locked out of the computer	6	19%

TABLE I
LABORATORY STUDY SUCCESS RATES

FACTOR USABILITY (GOOGLE)

🥇 U2F & Push

Had the fastest median authentication times

Compared to SMS [Duo research]:

- Push saves a user **13 minutes annually**
- U2F saves a user **18.2 minutes annually**

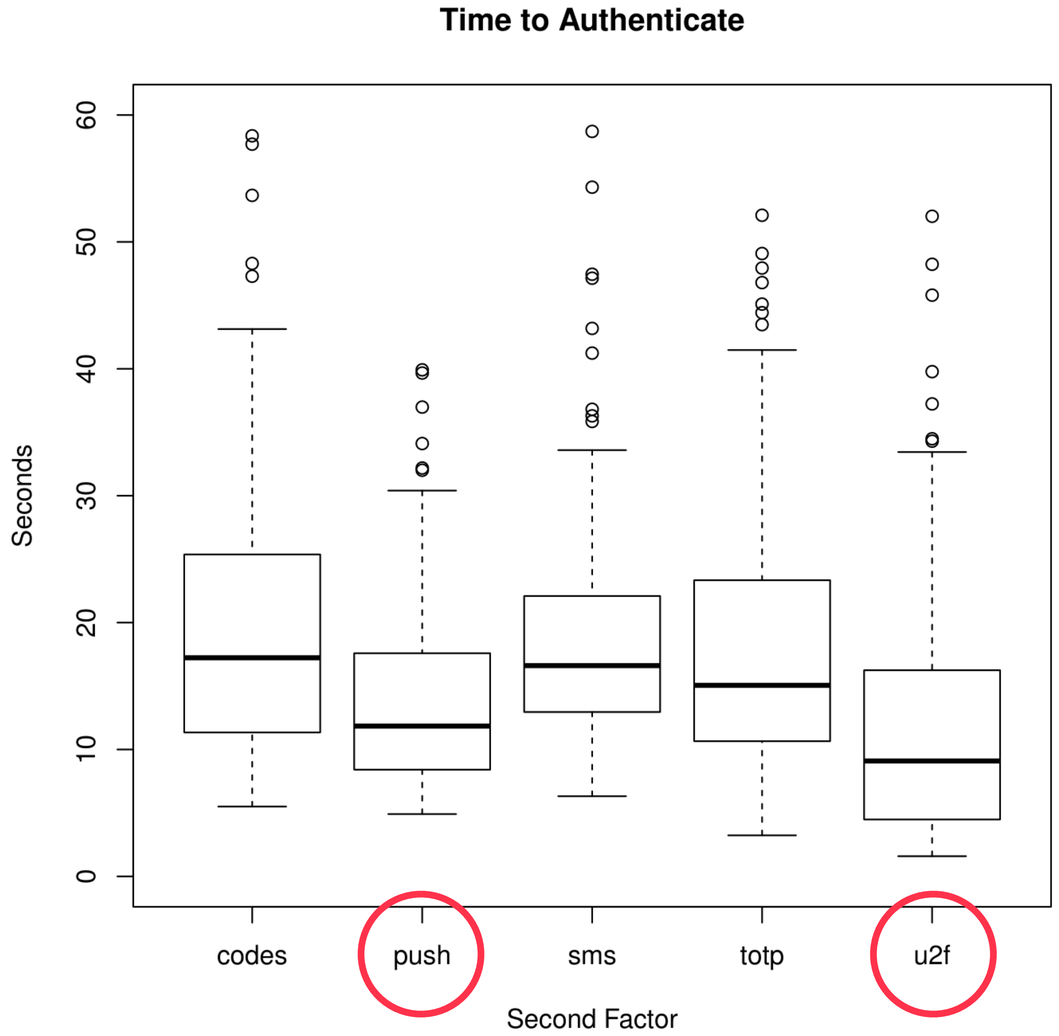


Figure 2: Time to authenticate for five 2FA methods

https://www.usenix.org/system/files/soups2019-reese.pdf

Duo 2019 State of the Auth Report

FACTOR USABILITY (GOOGLE)

🏅 TOTP

scored the highest System Usability Scale (SUS) score for a 2nd factor

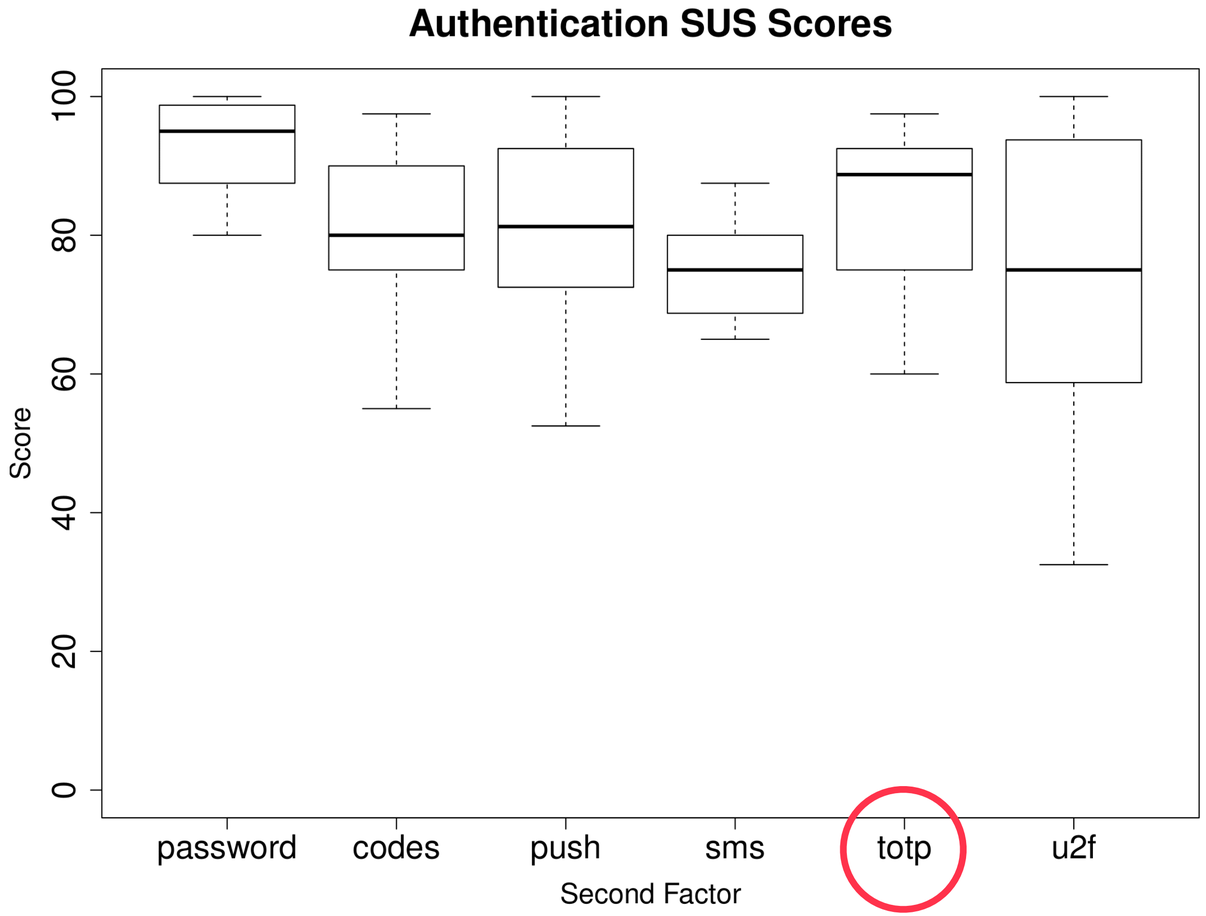


Figure 3: SUS scores for five 2FA methods.

https://www.usenix.org/system/files/soups2019-reese.pdf

FACTOR USABILITY (GOOGLE)

📉 U2F & Push

"Faster authentication does not necessarily mean higher usability"

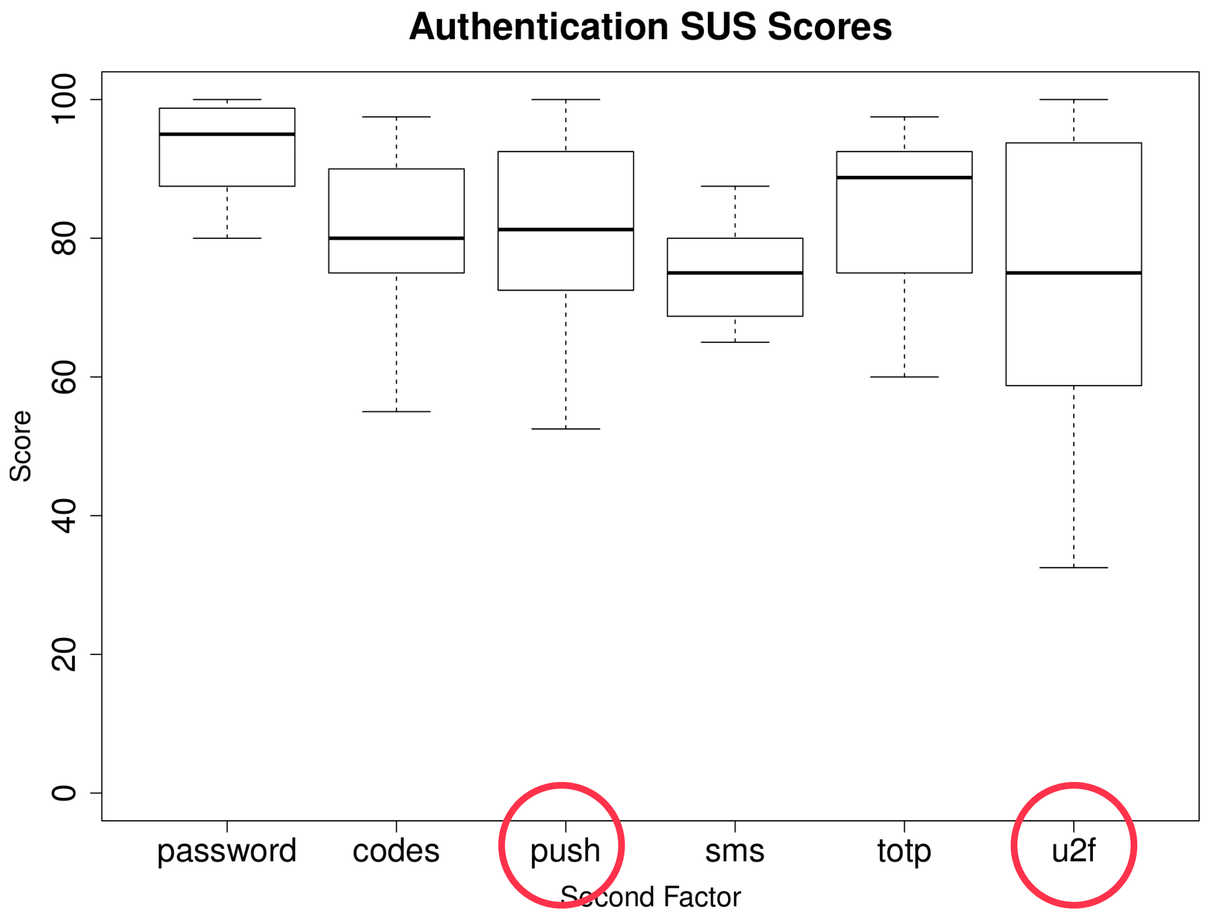


Figure 3: SUS scores for five 2FA methods.

https://www.usenix.org/system/files/soups2019-reese.pdf

SMS 2FA is still
better than **no 2FA**

SMS 2FA

2019 Google study found **SMS 2FA effectively blocks:**

100%

AUTOMATED BOTS

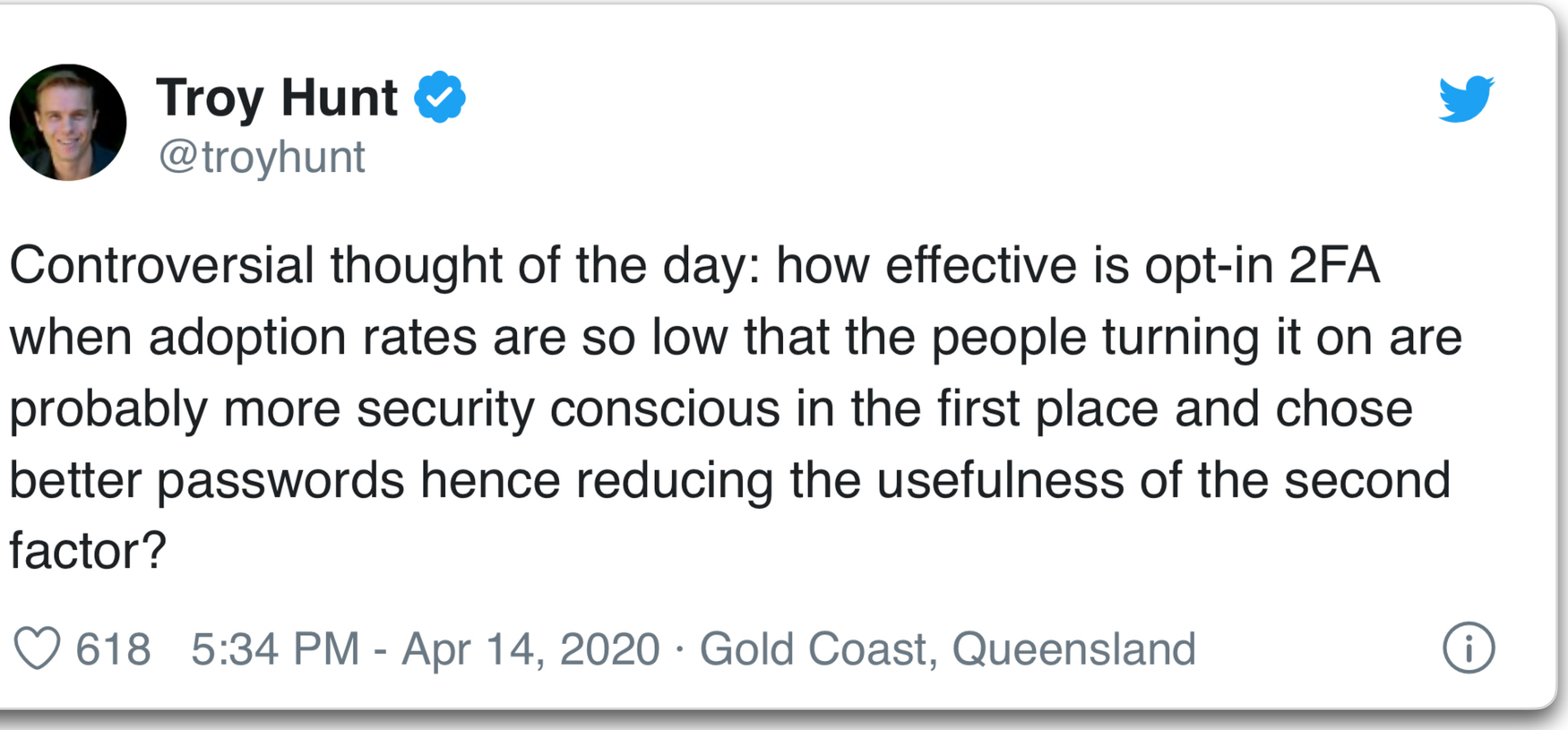
96%

BULK PHISHING ATTACKS

76%

TARGETED ATTACKS

https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html



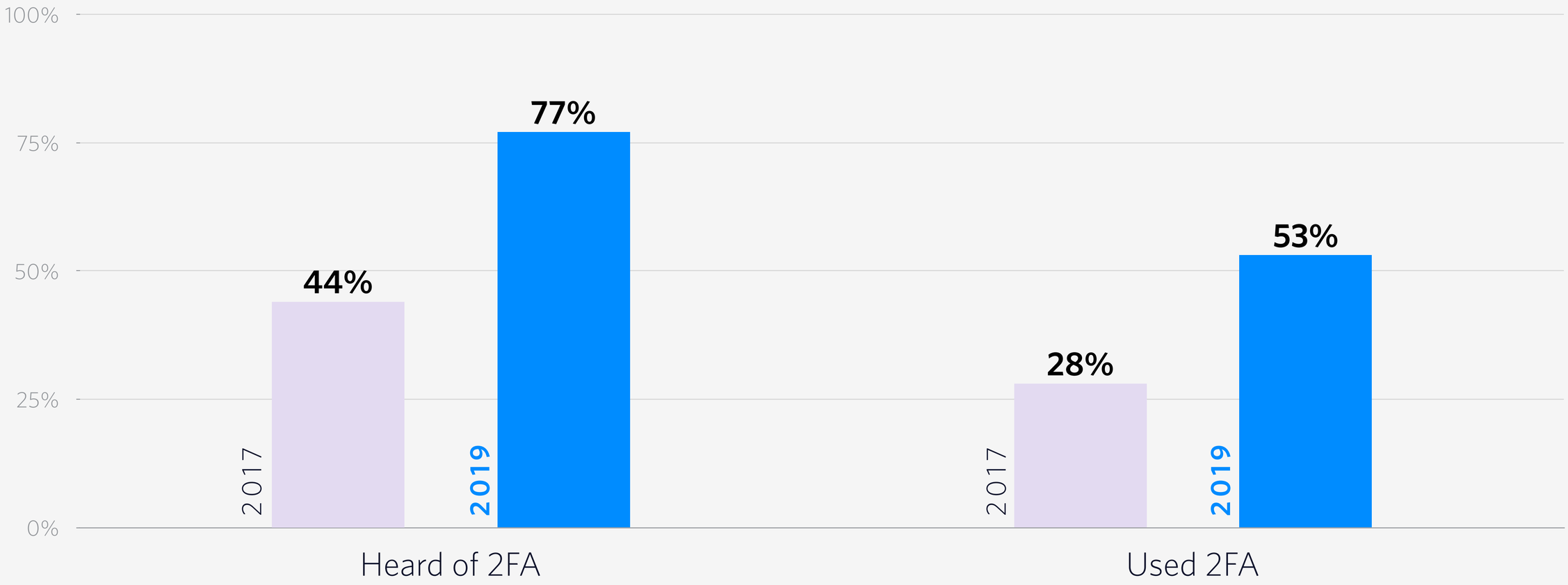
https://twitter.com/troyhunt/status/1250175511952683008

Perceived value of 2FA

> “I just don’t think I have anything that people would want to take from me, so I think that’s why I haven’t been very worried about it.”

Research participant | **A Usability Study of Five Two-Factor Authentication Methods**

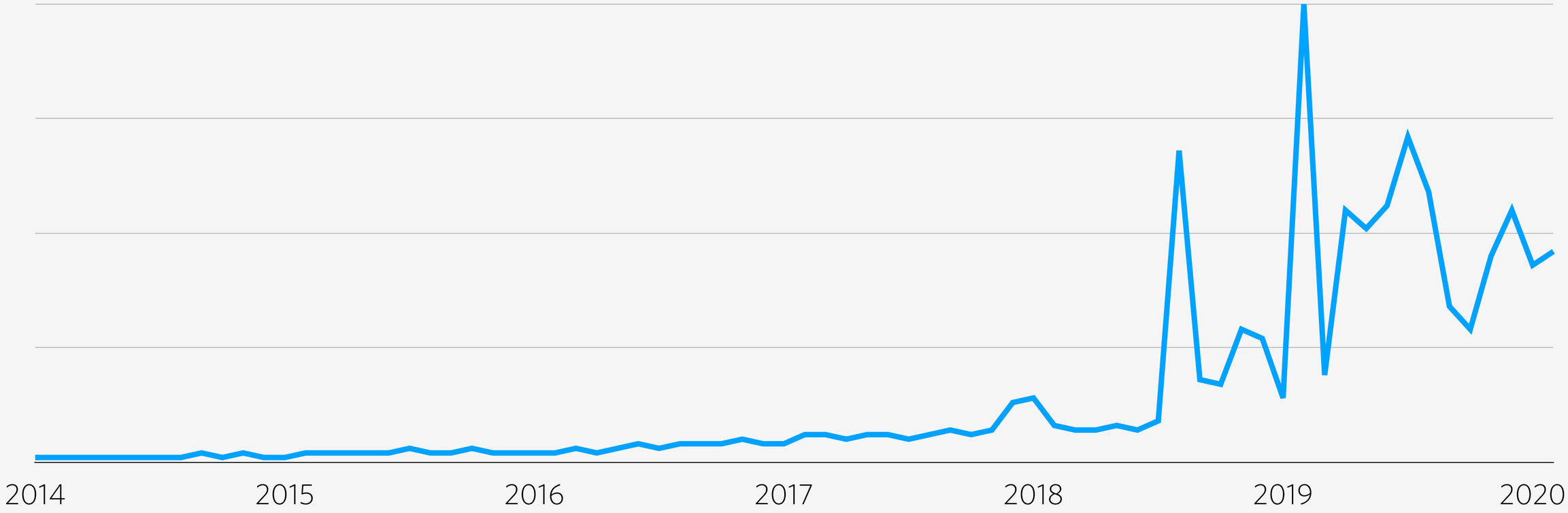
2FA ADOPTION (2017 VS. 2019)



Source: Duo 2019 State of the Auth Report

How to drive adoption of MFA

2FA GOOGLE SEARCH INTEREST OVER TIME (US)



Source: Google Trends

2FA GOOGLE SEARCH INTEREST OVER TIME (US)

Source: Google Trends

TechCrunch: Epic Games 2FA

2FA GOOGLE SEARCH INTEREST OVER TIME (US)

Source: Google Trends

TechCrunch: Epic Games 2FA

ENABLE 2FA

Two-Factor Authentication (2FA) protects your account. Enable 2FA to get the Boogie Down emote!

Enable 2FA Now

Remind Me Later

Never Show Again

Related queries

1	fortnite 2fa
2	fortnite
3	enable 2fa
4	enable
5	epic 2fa

MEASURING SUCCESS

MEASURING SUCCESS

💰 Losses due to account takeover ⬇️

😈 Number of compromised accounts ⬇️

ℹ️ Support costs relative to losses ⬇️

😀 User satisfaction ⬆️

Delight your most security conscious users.

Provide options for the rest.

"When we exaggerate all dangers we simply train users to ignore us."

Cormac Herley, **The Rational Rejection of Security Advice by Users (2009)**

THANK YOU

@kelleyrobinson

References

A usability study of five two-factor authentication methods

A Tale of Two Studies: The Best and Worst of YubiKey Usability

Javelin Strategy & Research, 2019

Duo 2019 State of the Auth Report

New research: How effective is basic account hygiene at preventing hijacking

Google Trends: 2FA (US)

TechCrunch: Epic Games 2FA