

---

Duo Labs Report

# State of the Auth

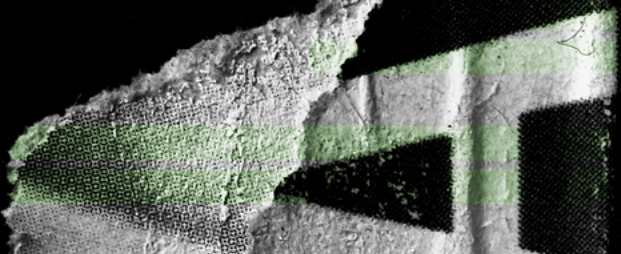
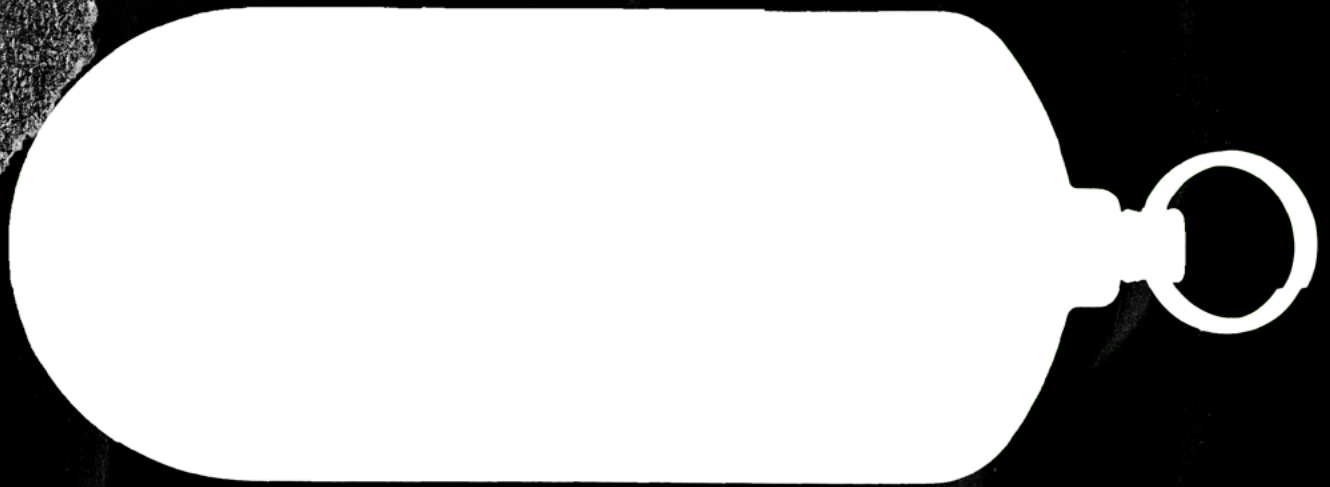
Experiences and Perceptions  
of Multi-Factor Authentication

**2021**

**DUO LABS**



TK



# State of the Auth

## Experiences and Perceptions of Multi-Factor Authentication

### Table of Contents

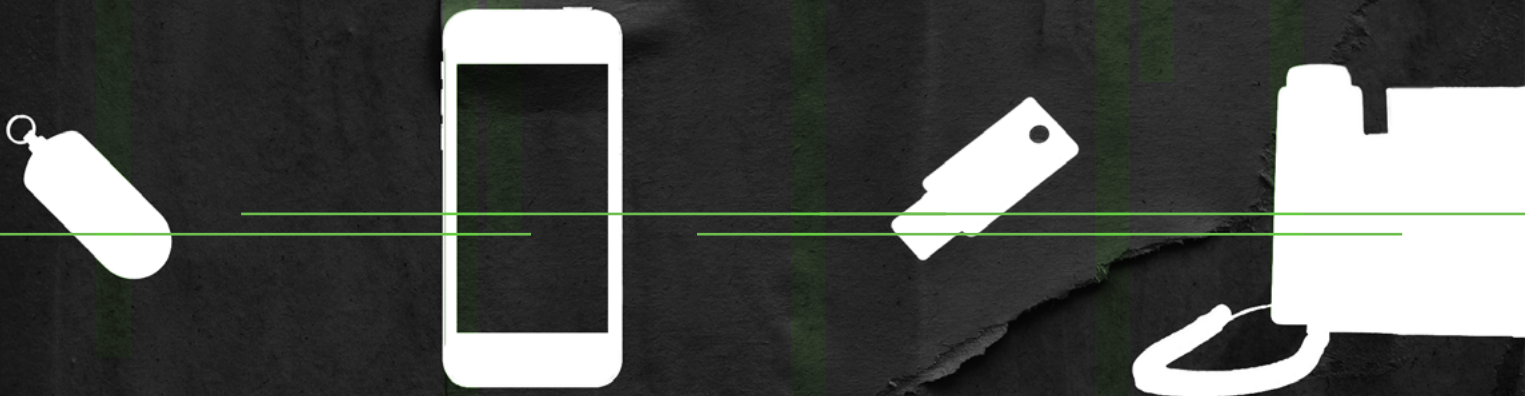
**AUTHOR**

Dave Childers

**PUBLISHED**

September 14, 2021

<b>1.0 OVERVIEW</b>	<b>1</b>
<b>2.0 KEY FINDINGS</b>	<b>3</b>
<b>3.0 DISCUSSION</b>	<b>7</b>
<b>4.0 REFERENCES</b>	<b>8</b>
<b>5.0 APPENDIX</b>	<b>9</b>



1.0

# Overview

Two-Factor Authentication (2FA) is a method of granting access to an application by requiring a user to present two pieces of verification, also called factors. Commonly, the first authentication factor is something that a user knows (such as a username and password pair), and the second factor is something that a user has (such as a phone or hardware token).

According to Verizon's Data Breach Investigation Report,<sup>1</sup> approximately 61% of security breaches involve compromised passwords. While not a silver bullet, 2FA has been shown to be effective in reducing the success rate of account takeover.<sup>2</sup>

Duo conducts a biennial, census-representative survey to understand the adoption of 2FA in the United States and United Kingdom.<sup>3,4</sup>

In this survey, we ask respondents about their experiences with 2FA and their perceptions around usability and security. This report will drill down on the following 2FA factors:



Second Factor	Definition
Short Message Service (SMS)	A code sent to a phone via text message
Email	A code sent to an email address
Phone Call	A call that provides authentication instructions
Push Notification	A message sent by an app prompting you to confirm or deny access to an application
Mobile Passcode	A verification code displayed by a 2FA Mobile App
Hardware Token	A standalone piece of hardware that displays a code
Security Key	A small device connected to a computer that verifies your identity via touch. Note, this is not the same as a built-in biometric such as FaceID or TouchID

The report also explores new trends in primary authentication, including password managers and biometrics. A password manager is a computer program that allows users to store, generate and manage their passwords. Common password managers include 1Password, LastPass, and Bitwarden.

Biometric authentication provides access to an application by verifying a physical characteristic of the user, such as fingerprint or facial recognition. Examples include Apple's Face ID and Touch ID.

## Methodology

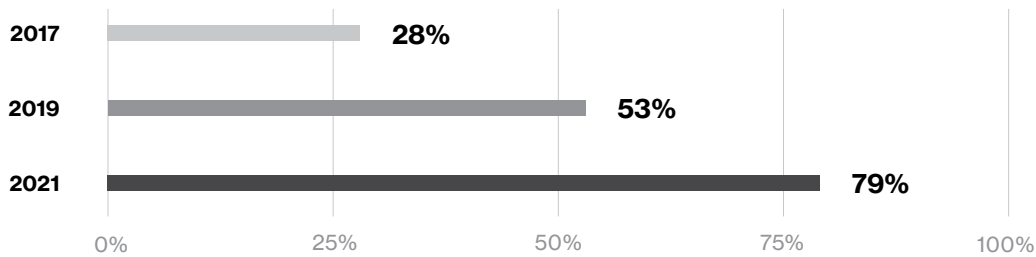
To understand individuals' experience and perception of 2FA, Duo designed a census-representative survey of 1,039 adults in the United States and United Kingdom. In order to ensure an accurate representation of the larger adult population, survey participants were balanced on sex, age, race, education, and country. The survey was administered by Qualtrics. Checks such as response speed were enforced to ensure response quality.

The survey used a seven-point Likert scale (1: strongly disagree, 7: strongly agree) to measure perceptions about the usability and security of 2FA factors. The 2019 report combined email and social media accounts when asking respondents about 2FA behavior. These account categories are separated for the current report. To assess differences in 2FA usage among demographic groups, chi-square tests of independence were used.

# Key Results

## Finding 1:

Have you used 2FA?





Two-factor authentication has become substantially more prevalent over the last two years, with 79% of respondents reporting having used 2FA in 2021.

## Finding 2:

Adoption of 2FA is significantly higher in the UK (77%) than the US (67%). The report from 2019 indicated no significant difference between the two countries, but the data indicated a similar trend to current findings. Country differences may be explained by discordant regulatory standards for 2FA adoption. Furthermore, this survey finds UK respondents more likely to agree with the statement, "I worry that hackers or other malicious actors could gain access to my accounts."



### 2FA ADOPTION BY COUNTRY

Country	# of Respondents	# Using 2FA	2FA Adoption Rate
UK	520	399	77% 
US	519	350	67% 

### Finding 3:

There are modest differences in 2FA adoption rates across age groups. There are similar rates of 2FA adoption among all respondents under 65.

#### 2FA ADOPTION BY AGE

Age	# of Respondents	# Using 2FA	2FA Adoption Rate
18–24	83	60	72%
25–34	227	170	75%
35–44	307	231	75%
45–54	194	134	69%
55–64	129	95	74%
65+	99	59	60%

### Finding 4:

There is an association between employment status and 2FA adoption, with adoption of 2FA nearly 20% higher among respondents who are currently employed.

#### 2FA ADOPTION BY EMPLOYMENT

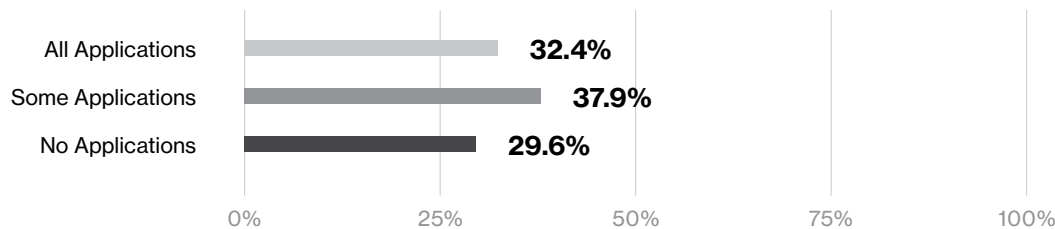
	# of Respondents	# Using 2FA	2FA Adoption Rate
Employed	670	528	79%
Unemployed	369	221	60%

### Finding 5:

Adoption of 2FA remains inconsistent across applications. For example, some respondents may enable 2FA on their bank account but not their email. While the number of respondents using 2FA for at least *some* applications has shown a sharp increase between 2017 and 2021, only a minority of respondents (32%) report using 2FA on all applications that offer it.



#### HOW DO USERS ENABLE 2FA ACROSS ACCOUNTS AND APPLICATIONS

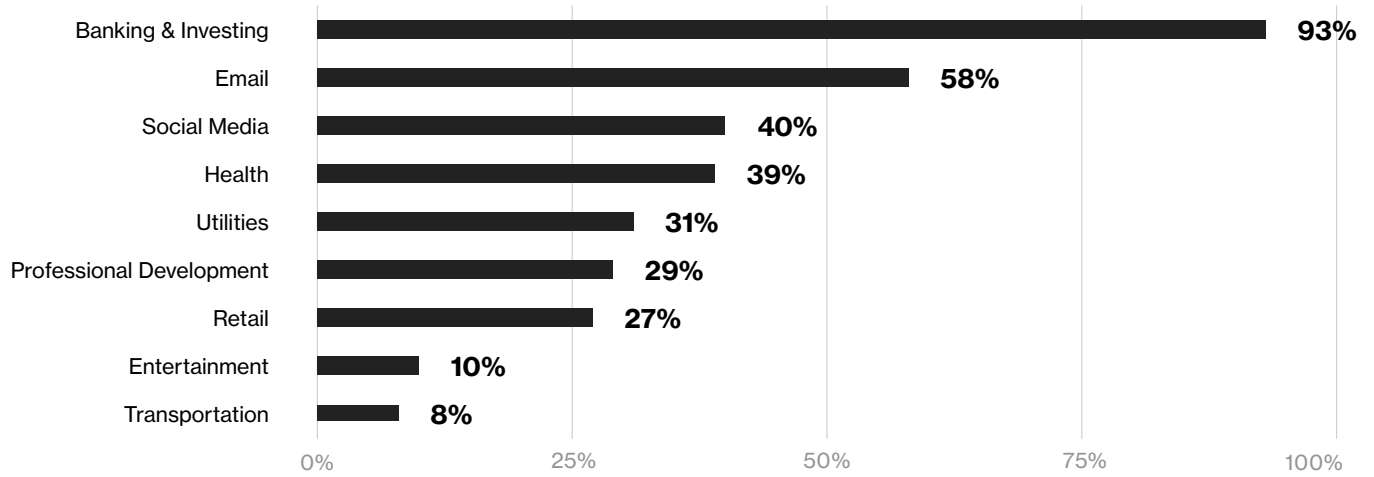


### Finding 6:

Respondents ranked financial accounts as the account category of highest concern should an unauthorized person gain access. Email and social media accounts ranked second and third, respectively, as the most important account categories to protect. There is evidence, however, that the impact of an email compromise is more harmful than a financial account compromise.<sup>5</sup>

#### ACCOUNT IMPORTANCE BY CATEGORY

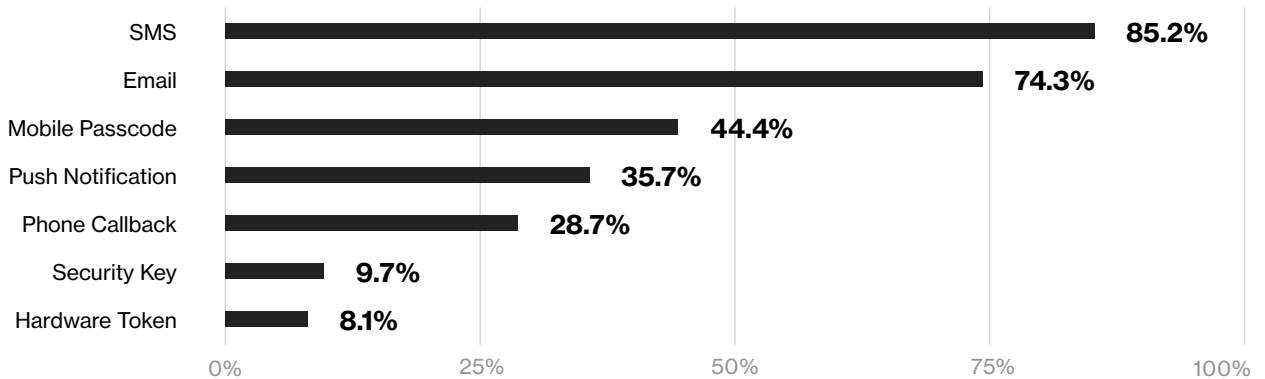
RESPONDENTS COULD SELECT UP TO 3



### Finding 7:

SMS (85%) continues to be the most common second factor that respondents with 2FA experience have used, with email the second most common second factor (74%).

#### WHICH SECOND FACTORS HAVE YOU USED?

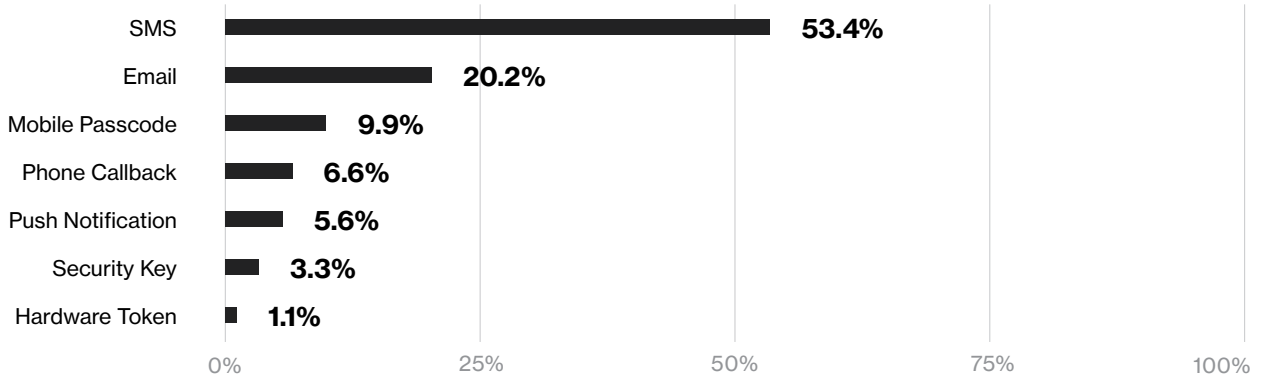




### Finding 8:

SMS is by far the most common choice among respondents for the second factor they would choose for a new account (53%), more than double the second most common choice of email (20%).

#### WHICH SECOND FACTOR WOULD YOU ADOPT FOR A NEW ACCOUNT?



### Finding 9:

Respondents rated SMS as the most usable second factor, and there is very little variation across factors in terms of security perceptions. A preference for SMS likely reflects the prevalence of SMS as a second factor, as evidence suggests it is one of the least secure second factors.<sup>6</sup>

#### PERCEIVED SECURITY & USABILITY OF 2FA FACTORS AMONG RESPONDENTS USING EACH FACTOR

Factor	Overall Usability*	Security	# of Respondents
SMS	5.46	5.73	697
Mobile Passcode	5.27	5.66	363
Push	5.27	5.49	292
Email	5.19	5.68	608
Phone	4.84	5.45	235
Security Key	4.83	5.73	79
Hard Token	4.42	5.68	66

\*Usability is a scale combining convenience, enjoyment, frustration and necessary instructions.

### Finding 10:

Biometrics and password managers are emerging important trends in primary authentication. In this survey, 32% of respondents report using a password manager, and 42% report using biometric authentication for at least some applications.

# Discussion



Adoption of two-factor authentication has substantially increased over the last four years. In Duo's first State of the Auth report in 2017, only 28% of respondents reported having used 2FA. Four years later, 79% of respondents have used 2FA, with 72% of respondents currently using 2FA. However, considering only 32% of respondents report using 2FA on all applications where it is available, there is still ample opportunity to improve 2FA adoption.

Email is frequently a recovery mechanism for other accounts, and banks often have safeguards to prevent individual financial losses due to unauthorized access.<sup>5</sup> There is an opportunity to increase security via increasing public awareness of the importance of protecting email accounts.

SMS is expected to continue to be the dominant second factor beyond 2021, as individuals are most familiar with this method of 2FA and expect to choose SMS as their preferred 2FA method going forward. While SMS is certainly more secure than no 2FA, other factors, such as push notifications and security keys, are more effective in preventing account takeovers.<sup>6</sup> With 2FA becoming more ubiquitous, users need to be better informed about the security guarantees of different types of 2FA factors. Recent guidelines from the Democratic National Committee for securing devices and accounts explicitly discourage the use of SMS.<sup>7</sup>

Two contemporary trends in primary authentication are password managers and biometrics. Password managers are a tool which securely stores a user's existing passwords and can assist in the creation of new, more secure passwords. Instead of using something you know (username and password) as the primary factor, biometric authentication verifies identity with a user characteristic (such as a fingerprint). In a separate study conducted by Duo, the top two user privacy concerns about biometric authentication were attackers replicating a biometric (42%) and distrust of companies with personal biometric information (36%).

With 80% of employed respondents indicating they currently use 2FA on at least some applications, the workplace offers a compelling avenue to maximize the effectiveness of 2FA adoption. Workplace security education programs can reinforce 2FA best practices such as the importance of enabling 2FA on email and social media accounts. Education programs can also highlight the limited effectiveness of SMS as a second factor compared to more secure alternatives such as security keys and push notifications.

# References

- <sup>1</sup> *2021 Data Breach Investigations Report* (<https://www.verizon.com/business/resources/reports/dbir/>); Verizon; 2021
- <sup>2</sup> *New research: How effective is basic account hygiene at preventing hijacking* (<https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>); Google Security Blog; May 17, 2019
- <sup>3</sup> *State of the Auth 2017* (<https://duo.com/assets/ebooks/state-of-the-auth.pdf>); Duo Security; November 7, 2017
- <sup>4</sup> *State of the Auth 2019* (<https://duo.com/assets/ebooks/state-of-the-auth-2019.pdf>); Duo Security; December 9, 2019
- <sup>5</sup> *Account security: a divided user perception* (<https://elie.net/blog/security/account-security-a-divided-user-perception/>); February, 2019
- <sup>6</sup> *The Usability of Five Two-Factor Authentication Methods* (<https://www.usenix.org/system/files/soups2019-reese.pdf>); Usenix.org; August 2019
- <sup>7</sup> *Device and Account Security Checklist* (<https://democrats.org/wp-content/uploads/2020/07/Device-and-Account-Security-Checklist-2.0-v4-1.pdf>); Democratic National Committee; July, 2020

# Appendix

## Survey Questions & Demographics

Demographic Information: country, gender, age, ethnicity, level of education, employment

### Basic 2FA Use

- Do you use 2FA?
- How long have you used 2FA?
- Do you use 2FA on some or all of your applications?
- Why did you start using 2FA?

### Perceptions of Risks

#### **Account Security**

- Do you worry about hackers gaining unauthorized access to your accounts?
- Do you believe your accounts are generally secure?

#### **Passwords**

- Do you tend to select strong/complex passwords?
- Do you tend to select a unique password for each account?
- Do you use a password manager?
- Do you use biometrics to access some applications?

#### **Accounts by Sector**

- What online accounts do you use (by sector)?
- For which categories of accounts would you be most concerned about a person gaining unauthorized access?

#### **Second Factor Methods**

- Which of the following authentication factors do you think would be easiest to use?
- Which do you think would be the most secure?
- Which would you be most likely add to a new account and why?
- Which would you be least likely to add to a new account and why?
- Which 2FA factors have you used before? For each factor you have used, the degree to which you agree the factor was:
  - Convenient
  - Enjoyable
  - Required instructions
  - Frustrating
  - Secure

**Table:** 2FA Usage and Respondent Demographics

**STATISTICAL TESTS OF ASSOCIATION WITH 2FA USE**

CHI-SQUARE TESTS OF INDEPENDENCE

Demographic	# of Groups	df	statistic	p-value
Country	2	1	10.692	0.001
Age	6	5	11.117	0.049
Employment	2	1	41.373	0.000

## About the Author

### Dave Childers

@dmchilders

#### Data Scientist

Dave Childers is a Data Scientist at Duo Security. Prior to Duo, Dave worked in data science at various organizations in both the academic and private sectors since completing his master's degree in statistics at the University of Michigan.

