State of the Auth

Experiences and Perceptions of Multi-Factor Authentication
State of the Auth

Experiences and Perceptions of Multi-Factor Authentication
Introduction

Two-factor authentication (2FA) has been proven to be highly effective in preventing and deterring account takeover. In a year-long study by Google, the addition of a second factor to the authentication flow thwarted 100% of challenges by automated bots, which used password dumps to try to brute-force credentials. On-device prompts similar to Duo Push stopped 99% of bulk phishing attacks and 90% of targeted attacks (phishing emails designed specifically to appeal to the intended victim); SMS codes stopped 96% of bulk phishing attacks and 76% of targeted attacks; and security keys stopped 100% of both bulk phishing attacks and targeted attacks.1 At Duo, we recognize the benefits of 2FA, as do our customers. Security is our mission, and it is top-of-mind for our customers trying to protect valuable corporate assets. But we wanted to find out how the average person views 2FA—or whether that user even knows about it.

In 2017, Duo Labs, the security research team at Duo Security, conducted a census-representative survey to measure the adoption of the 2FA in the United States, and the perceptions of Americans on different 2FA technologies and delivery methods.2 At that time, we found that 28% of Americans used 2FA on at least one website or application. Over half of the respondents, about 56%, had never heard of 2FA prior to the survey.

A lot has changed in the two years since this inaugural survey: Apple announced and released Face ID on its iPhone X, becoming the first to provide secure authentication via facial recognition.3 The Global Data Protection Regulation (GDPR) became fully enforced through the European Union after its grace period ended in May 2018.4 Most recently, the WebAuthn web standard was published as a World Wide Web Consortium (W3C) recommendation, paving the way for secure web authentication via public key cryptography.5 Because of this quickly changing landscape, we felt an imperative to understand the current attitudes towards 2FA, and how they compare to our previous results.
Related Work

The survey conducted for this report was based on the 2017 State of the Auth survey, which in turn drew inspiration from A Comparative Usability Study of Two-Factor Authentication\(^1\) and How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior.\(^2\) These related studies have sought to answer questions about which authentication factors are easiest to use, and where people receive information about security practices. De Cristofaro et al. claim that the key factors that affect 2FA usability can be boiled down to ease-of-use, required cognitive efforts, and trustworthiness. More recently, Reese et al. measured several aspects of usability among five different authentication factors on the same platform, including time to setup and time to authenticate.

Methodology

To build on this body of research, we asked questions about the usage and experience of several authentication factors, as well as questions about perceived security and value. In the 2017 iteration of this survey, 28% of all respondents had used two-factor authentication. Respondents answered questions only about factors they had used, commenting on ease-of-use, required cognitive efforts, and trustworthiness among other metrics on the Likert scale. For this iteration, we also gathered information about the perceived notions of authentication factors, even for respondents who hadn’t used them. In addition, we added sections on more general security beliefs and behaviors.

Survey

Prior to the survey, cognitive interviews were conducted to ensure that the questions were worded in a clear manner, and that each authentication factor was adequately described. The survey was conducted by Qualtrics, a third-party provider that sought out a sample of participants that were representative of the United States and United Kingdom populations in terms of age, ethnic background, education, and income according to the most recent census data for each respective country. Responses that were incomplete were excluded, and answer choices for each question besides demographic questions and those with Likert scale answer choices were randomized to mitigate order bias.

Our sample was largely representative of the respective geographic regions in terms of ethnicity, education, and household income distributions. However, the original sample from the United States was 62% female and 38% male, while the sample from the United Kingdom was 65% male and 35% female. As a result, the overall group was fairly gender-balanced, but each region was somewhat skewed. To correct for this imbalance, each statistic reported is computed on a subsample of the data associated with each country, where the subsample proportions match census estimates.
Key Results

Have you heard of 2FA?

<table>
<thead>
<tr>
<th>Year</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>44%</td>
</tr>
<tr>
<td>2019</td>
<td>77%</td>
</tr>
</tbody>
</table>

77% of people have heard of 2FA, up from 44%. Of those who weren’t already using 2FA, more than half had never heard of it, meaning that while the visibility of two-factor authentication has grown substantially in the past two years, there’s still opportunity for increased awareness.

Have you used 2FA?

<table>
<thead>
<tr>
<th>Year</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>28%</td>
</tr>
<tr>
<td>2019</td>
<td>53%</td>
</tr>
</tbody>
</table>

53% of people use 2FA, up from 28%. The majority of the respondents in our survey used at least some type of two-factor authentication.
More secure factors like push notifications and security keys are well-liked...by those who've used them. In the U.S., security keys rated highest for both perceived security and enjoyment, but just 12% of those who use 2FA had used a security key to authenticate. Push notifications were rated second-highest in enjoyment, as well as the least frustrating authentication factor, based on the 19% of total 2FA users who use push notifications.

Banking and investment accounts ranked most important to protect. Across the board, people were most concerned about protecting banking and investment accounts, despite the consequences potentially being more severe for account takeover of email or social media. 7

There was no statistical difference between adoption of 2FA in the United States and in the United Kingdom. However, the Americans surveyed were 5% more likely to strongly agree with the statement, "I worry about malicious actors gaining access to my accounts."

SMS messaging is still the authentication factor that most people have used. Although the security flaws of SMS are well-documented, it remains the authentication factor that most respondents had used, with 71.5% having experienced authentication via SMS message. Its prevalence could be due to SMS not requiring an app on the end-user device, and working on non-smartphones.

12% Have used a security key.

71.5% Have experienced 2FA via SMS.
SMS messages remain most common, followed by email. SMS messages were also the most popular choice for a question that asked participants to select their preferred authentication factor for a hypothetical new account. It appears that widespread familiarity with SMS has bred a high level of comfort as compared to other, more secure factors. However, users who had tried other means of 2FA, like push notifications, authenticator apps, and security keys, rated them nearly as convenient.

The halo effect around SMS messaging produced another interesting result, which is that it had the highest proportion of users agree with the statement "Using it was quick." Push notifications and U2F tokens, which took second and third, are the fastest authentication methods on average. The median time to authenticate for these factors beat that of SMS messages by five and seven seconds respectively.

A lower proportion of 2FA users had authenticated with a hardware token than previously measured, continuing the downward trend observed in our last State of the Auth for the authentication factor, which came in last in ratings of convenience and usability.

### 2FA Usage

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>2019</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS</td>
<td>72%</td>
<td>86%</td>
</tr>
<tr>
<td>Email</td>
<td>57%</td>
<td></td>
</tr>
<tr>
<td>Authenticator App (OTP)</td>
<td>36%</td>
<td>52%</td>
</tr>
<tr>
<td>Phone Callback</td>
<td>30%</td>
<td>39%</td>
</tr>
<tr>
<td>Push Notification</td>
<td>18%</td>
<td>33%</td>
</tr>
<tr>
<td>Security Key</td>
<td>13%</td>
<td>19%</td>
</tr>
<tr>
<td>Hard Token</td>
<td>10%</td>
<td>9%</td>
</tr>
</tbody>
</table>

*In our 2017 survey, Email and SMS were combined into a single selection. We decided to separate them for 2019’s survey.*
2FA Usage Demographics

The strongest indicator of whether or not any single respondent was a user of 2FA was the individual’s self-reported knowledge of information security. Of those who referred to themselves as unfamiliar with the subject, 22% had used 2FA; the beginners, 40%; those who claimed intermediate knowledge, 65%; and a full 83% of self-reported experts in information security were 2FA users. These trends were also observable by looking at the age of the respondents. In general, younger respondents were more likely to consider themselves knowledgeable about information security and also more likely to use two-factor authentication.

2FA Usage by InfoSec Knowledge
(Self-reported)

<table>
<thead>
<tr>
<th>Knowledge Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unfamiliar</td>
<td>22%</td>
</tr>
<tr>
<td>Beginner</td>
<td>40%</td>
</tr>
<tr>
<td>Intermediate</td>
<td>65%</td>
</tr>
<tr>
<td>Expert</td>
<td>83%</td>
</tr>
</tbody>
</table>

2FA Usage by Age

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-24</td>
<td>69%</td>
</tr>
<tr>
<td>25-34</td>
<td>68%</td>
</tr>
<tr>
<td>35-44</td>
<td>58%</td>
</tr>
<tr>
<td>45-54</td>
<td>49%</td>
</tr>
<tr>
<td>55-64</td>
<td>36%</td>
</tr>
<tr>
<td>65+</td>
<td>33%</td>
</tr>
</tbody>
</table>
Security Behaviors

In this section of the survey, participants were asked to read a statement and select an option from “Strongly disagree,” “Disagree,” “Somewhat disagree,” “Neither agree nor disagree,” “Somewhat agree,” “Agree,” and “Strongly agree.” We report on individual response rates as well as agreement (the sum of “Somewhat agree,” “Agree,” and “Strongly agree”) and disagreement (the sum of “Somewhat disagree,” “Disagree,” and “Strongly disagree”) in general.

Thirty-nine percent of respondents in the United States strongly agreed with the statement “I worry that malicious actors could gain access to my accounts,” while only 25% of respondents in the United Kingdom did. The total proportion that selected some form of agreement was about 80% in both groups.

Twenty-six percent of respondents in the United States selected “Agree” for the statement “I believe that my accounts are generally secure,” as did 38% of respondents in the United Kingdom, making it the most common response. Overall, about 74% of Americans and 78% of Britons think their accounts are generally secure (choosing any of the three agreement responses).

Interestingly, the responses to the statement “I tend to select strong, complex passwords” was very similar across the two regions (32% and 35% agree in the U.S. and U.K. respectively), but Americans were more likely to strongly agree with the statement “I tend to select a unique password for each of my accounts.” (33% as compared to 22%). A very low proportion disagreed with these statements, which based on previous password research is likely an example of social desirability bias. In our study, just 7% in the United States and 8% in the United Kingdom expressed any form of disagreement with “I tend to select a unique password for each of my accounts” – a recommended behavior for security hygiene. A study of password dumps estimated 43% of study participants reuse passwords.

6
Online Account Usage

In another section, survey participants were asked to select up to three online accounts that they were most concerned about protecting. Surprisingly, Communications and Social Media was not the response most frequently selected by participants, coming out to about 32%. Since more people responded that they used online accounts for Banking and Financial Services, it’s possible that email was not interpreted as falling under the Communications category (as an email address is a prerequisite for many of the other categories).

Account Importance by Type

<table>
<thead>
<tr>
<th>Account Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking &amp; Finance</td>
<td>85%</td>
</tr>
<tr>
<td>Communications &amp; Social Media</td>
<td>32%</td>
</tr>
<tr>
<td>Health</td>
<td>28%</td>
</tr>
<tr>
<td>Retail</td>
<td>25%</td>
</tr>
<tr>
<td>Utilities</td>
<td>24%</td>
</tr>
<tr>
<td>Career &amp; Prof. Development</td>
<td>16%</td>
</tr>
<tr>
<td>Entertainment &amp; Media</td>
<td>12%</td>
</tr>
<tr>
<td>Transportation</td>
<td>6%</td>
</tr>
</tbody>
</table>

Users were by far the most concerned with protecting accounts related to Banking and Financial Services: participants were allowed to select up to 3 categories, and this category was selected as high priority by 85% of respondents. For comparison, the next-highest category was Communications and Social Media at 32%. Users were in general least concerned with protecting their Transportation and Entertainment and Media accounts. For those who use 2FA on some services but not all of them, the most common differentiator is the perceived importance of that account, making it especially important to understand where values lie.
While the overwhelming majority of respondents selected Banking and Financial Services as the account they were most concerned about, in many cases it’s actually the email accounts that are the most valuable. This is a bit counterintuitive, and certainly thinking about a hacker wiping out our life savings invokes a fear response. Banks and other financial institutions often have protections in place for large or unusual transactions, but in the absence of another 2FA method, email is usually the source of identity. Consider it this way, for almost every account that was created using your email address, (including bank accounts, social media accounts, health accounts, and all the others) that email address also provides the mechanism for account recovery. In other words, if someone gained access to the email account, they could change the login credentials to myriad other accounts without raising an alarm.

One of the reasons that people may be less concerned with protecting their Entertainment and Media accounts is the high rate of account sharing in this sector. According to a Cordcutting.com survey of more than 1,000 video streaming service users, 15% of Netflix users and 19.2% of Hulu users were using another subscriber’s account for access. At the time of this writing, neither Hulu nor Netflix support any form of 2FA. Sixteen and a half percent of users of Amazon Prime Video, which does offer 2FA, also copped to using another subscriber’s account. Such practices are commonplace, and it would make sense that users would be more reluctant to add a second factor if others were also accessing their account. This could be solved, for example, by enrolling multiple devices for multiple authorized users. While the damage in Entertainment and Media may be more limited than with other accounts, users have reported takeovers and unauthorized charges to their credit cards. Netflix’s own security page recommends that users avoid password reuse to keep their account secure.
Survey Results Summary

Both use and general awareness of two-factor authentication and its security benefits are increasing. However, outdated methods of delivering 2FA with known weaknesses, such as codes via SMS messages, are still the most common implementations. Convenience reigns as a top priority for the end user. Fortunately, methods such as security keys are growing in popularity, and are considered by the majority of those who had experience with them to be quick, easy to use, and secure.

More broadly, users on both sides of the Atlantic worry about the specter of hackers gaining access to their accounts, but agree that their accounts are generally safe. Many respondents claimed to practice excellent security behaviors such as the use of complex and unique passwords, a statistic that is biased by self-reporting, but at least suggests that the "proper" behavior is well-known and understood.

Most who did not use 2FA had not yet been exposed to the concept. Of the minority of participants who used 2FA but then stopped, the most popular explanations were the inconvenience of a second factor and a perceived lack of value in the accounts associated with those websites or applications. But many users recognized that they did have a lot worth protecting online—especially in Banking and Financial accounts, but also in Communications and Social Media and a variety of other sectors. Some even refused our instructions to select their top priorities, noting "They’re all important." Of 1.1% of respondents who didn’t answer this question, 89% wrote something to that effect in the text box (about 1.0% of our total sample).

Overall, the data paints a nuanced picture of the decisions users make as they navigate security decisions. They believe that their passwords and accounts are mostly secure, but worry about unauthorized access; they have concerns about privacy, but value convenience. Most of all, the survey is the first to demonstrate that the majority of people in the regions we covered are using some form of two-factor authentication, a great achievement for multi-factor authentication providers and for account security worldwide.
Survey Questions & Demographics

Demographic Information: country, gender, age, ethnicity, level of education, household income, knowledge of information security.

Basic 2FA Use

• Do you use 2FA? How long have you used it? Do you use it on some/all/none and why?

• Why did you start using 2FA?

• Where did you learn about 2FA?

• Why don’t you use 2FA?

• Why did you stop using 2FA (if applicable)?

Perceptions of Risks

Account Security

• Do you worry about people 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?

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?

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?

• For which categories of accounts would you be least concerned about a person gaining unauthorized access?

• Which 2FA factors have you used before, and for each one, the degree to which you’d agree it was:
  • Convenient
  • Quick
  • Enjoyable
  • Happy to do it again
  • User-friendly
  • Required instructions
  • Required concentration
  • Stressful
  • Frustrating
  • Trustworthy
  • More secure than just a username and password
References

1 New reaserch: How effective is basic account hygien at preventing hijacking (https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html); Google Security Blog; May 17, 2019

2 State of the Auth (https://duo.com/assets/ebooks/state-of-the-auth.pdf); Duo Security; November 7, 2017

3 About Face ID advanced technology (https://support.apple.com/en-us/HT208108); Apple Support; September 19, 2019

4 The European Union Legislative Process (https://eugdpr.org/the-process/); EUGDPR.org

5 W3C approves WebAuthn as the web standard for password-free logins (https://venturebeat.com/2019/03/04/w3c-approves-webauthn-as-the-web-standard-for-password-free-logins/); VentureBeat; March 4, 2019

6 The Tangled Web of Password Reuse (http://www.jbonneau.com/doc/DBCBW14-NDSS-tangled_web.pdf); NDSS-Symposium.org; February 22, 2014

7 Account security - a divided user perception (https://elie.net/blog/security/account-security-a-divided-user-perception/); Elie.net; February 2019

8 The Usability of Five Two-Factor Authentication Methods (https://www.usenix.org/system/files/soups2019-reese.pdf); Usenix.org; August 2019

9 Social Desirability (https://methods.sagepub.com/reference/encyclopedia-of-survey-research-methods/n537.xml); Sage Research Methods; 2008


About the Author

Maggie Engler
@maggieengler

Data Scientist

Maggie is a Data Scientist at Duo Security as part of the Duo Labs team. Prior to Duo, Maggie worked for various security organizations in both the private and public sector, most recently at a cyber risk startup in the Bay Area. She studied electrical engineering and applied mathematics at Stanford University.