DUO LABS

State of the Auth 2019

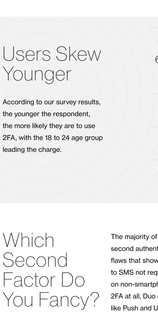
BY THE NUMBERS

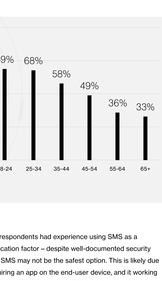
A data-driven look at how we authenticate.

Earlier this year, Duo Labs conducted a survey of people's use and perceptions of two-factor authentication (2FA). The team conducted a similar survey in 2017. Here are some key highlights from our *State of the Auth 2019* report.

Do You Even 2FA?

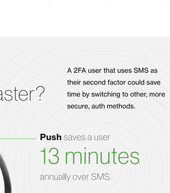
The amount of respondents who use and who have heard of 2FA is rising, a sign that security awareness is improving.





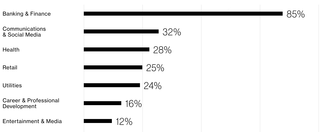
Users Skew Younger

According to our survey results, the younger the respondent, the more likely they are to use 2FA, with the 18 to 24 age group leading the charge.



Which Second Factor Do You Fancy?

The majority of respondents had experience using SMS as a second authentication factor – despite well-documented security flaws that show SMS may not be the safest option. This is likely due to SMS not requiring an app on the end-user device, and it working on non-smartphones. While using any form of 2FA is better than no 2FA at all, Duo recommends more secure authentication methods, like Push and U2F.



Tick Tock! Which Factor is Faster?

A 2FA user that uses SMS as their second factor could save time by switching to other, more secure, auth methods.

Push saves a user

13 minutes

annually over SMS.

U2F saves a user

18.2 minutes

annually over SMS.

Which Accounts Are Most Important?

We asked respondents which types of accounts are most important to protect. Not surprisingly, banking and financial was the runaway favorite.

Perceptions of Account Security

We asked respondents whether they agree with the statements:

"I worry about malicious actors **gaining access** to my accounts."

"I believe that my accounts are **generally secure**."

39% of **US** respondents **strongly agree**

25% of **UK** respondents **strongly agree**

74% of **US** respondents somewhat agree, agree or strongly agree

78% of **UK** respondents somewhat agree, agree or strongly agree

Positive Password Practices

We all know that passwords alone aren't the best protection - hence the need for 2FA. There are, however, some steps you can take to make your passwords stronger and better, such as making them unique and long, at least 16 characters in length. For the most part, survey respondents suggest they follow password best practices.

"I tend to select **strong, complex** passwords."

"I tend to select a **unique** password for each of my accounts."

To dive deeper into this data and more, download the *State of the Auth 2019* report from Duo Labs.

DUO LABS

@duo_labs
duo.com/labs