


DUO LABS

 Duo Security is
now part of Cisco.

Duo Labs Report

State of the Auth

Experiences and Perceptions
of Multi-Factor Authentication

State of the Auth

Experiences and Perceptions of
Multi-Factor Authentication

AUTHORS

Olabode Anise
Kyle Lady

EDITOR

Thu T. Pham

DESIGNER

Chelsea Lewis

PUBLISHED

11/7/2017

Table of Contents

1.0	Overview	1
2.0	Results	3
3.0	Conclusion	9



1.0 —

Overview

Duo Labs, the security research team at Duo Security, conducted user-focused research investigating the adoption of two-factor authentication (2FA) and users' perceptions of the different 2FA technologies and delivery methods.

Methodology

To measure perception and adoption, we administered a survey to a census-representative population. We chose this sample so we could understand how the average person in the United States views 2FA. Our findings help inform the broader security community so that we can better protect users through improved education and more usable products.

Process

In addition to the results of the study, we want to share our process of coming up with an idea and creating the survey that was used to obtain the results. Below, we've outlined the actions we took prior to the release of the survey.

Literature Review

Like any academic research project, we kicked things off by doing a literature review. A literature review is usually done prior to the start of a project so that you can understand what has already been done in the space, questions that still need to be answered, and things that could be improved upon. We conducted the literature review for this project over the course of two weeks, during which we reviewed existing research concerning two-factor authentication adoption and perception.

Our final study design came from the following papers:

“A Comparative Usability Study of Two-Factor Authentication”

and **“How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior.”** Similar to the methodology used in the first paper mentioned, we decided to conduct a census-representative survey and then ask about the 2FA methods currently available to improve on the study, similar to the second paper.

Survey Creation and Survey Testing

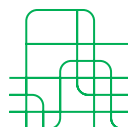
As expected, this proved to be the longest portion of the entire process. Since we were trying to make a comparison to a previously conducted survey, we didn't have to make all of the questions from scratch. We were able to utilize some of the questions from both of the papers that were previously mentioned while also adding some of our own.

In order to make sure that our survey questions were understandable, we enlisted the help of a few Duo employees to review our survey questions. Then we had people inside and outside of Duo take the survey. It is important to note that we didn't just conduct a pilot. We had participants take the survey, but we asked them follow up with questions about the questions asked and the answer choices so that we could identify any ambiguity or problems. This served as a replacement for cognitive interviews which have become standard when conducting surveys.

After our faux cognitive interviews, we enlisted the help of our friends in the usable security and human-computer interaction space to review our survey one last time. The edits made from their comments were the questions that were used in the survey.

Survey Platform and Sample Acquisition

In order to obtain a representative sample, we used Survey Sampling International. Per our request, they were able to provide a sample of 579 individuals comprised of a demographic breakdown that was based on the U.S. Census quotas for age, gender, race and income. Participants were directed to our survey that was administered via Qualtrics. In order to prevent **order bias**, we randomized answer choices for each question excluding the ones that included Likert items and those that were related to demographics.





2.0 ———

Results

In order to ensure the accuracy of our survey results, we included an attention check question: “Please choose very unhappy.” Attention check questions were included in order to ensure that participants maintained a consistent level of focus throughout the survey and that we received the highest quality answers. Only responses from the 443 participants who correctly chose “very unhappy” when prompted were included in the analysis below.

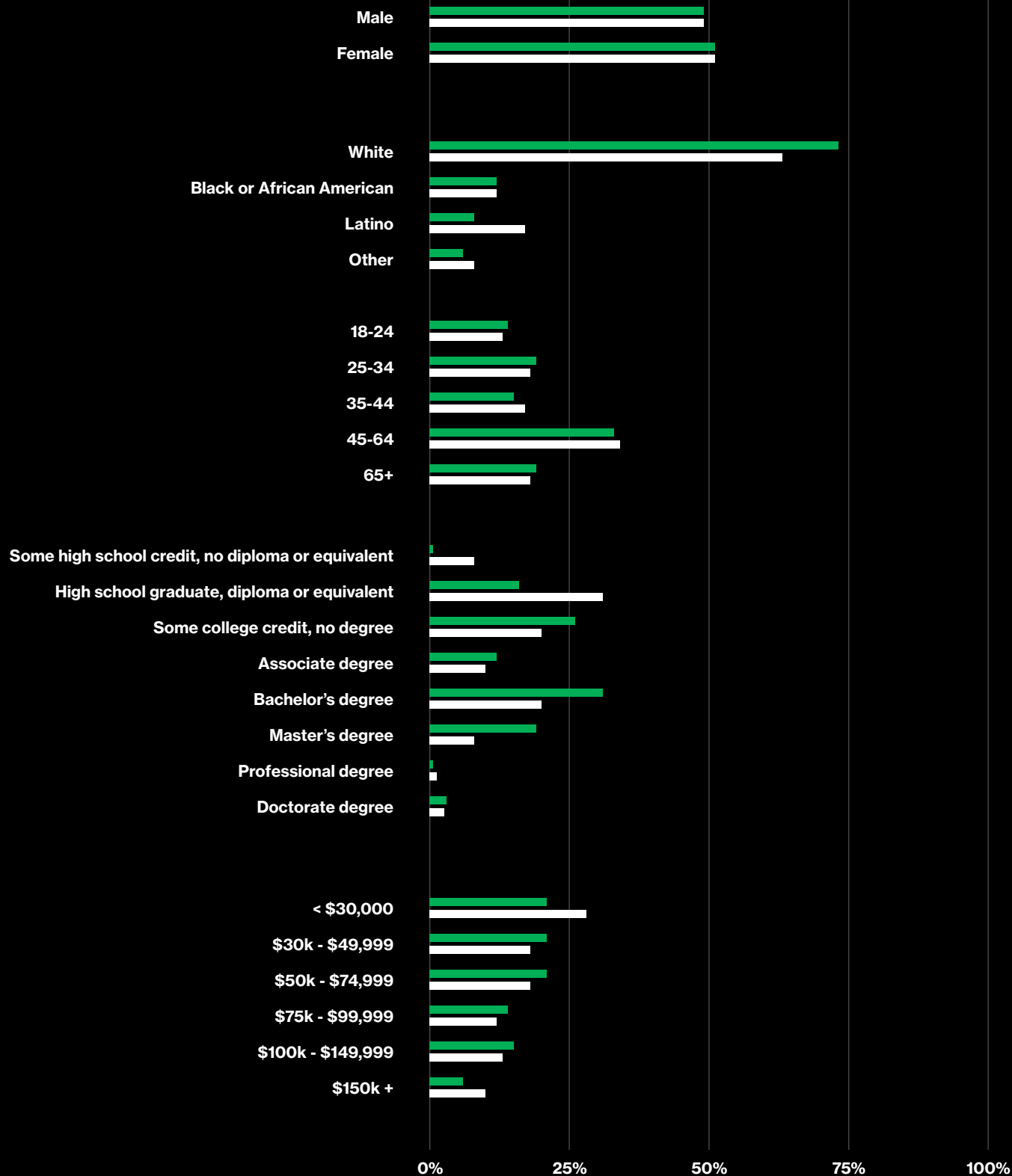
Participant Demographics

When assessing how closely our survey sample compares to the general United States population, we decided to use the 2015 American Community Survey five-year estimates. By using this particular set of data, we have traded currency for increased precision and a larger sample size.

In regards to gender and age, our survey sample is very representative of the U.S. population. However, our population proved to be wealthier, more educated and composed of more white participants than the U.S. average.

Participant Demographics

■ Sample
■ US Census



General Use of 2FA

We hypothesized that the majority of the US doesn't use 2FA. While gut feelings are good, actual numbers are always better. So after explaining what 2FA is, we asked our survey participants "Do you currently use 2FA?"

Our survey results found that:

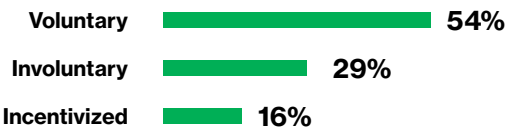
- **Only 28% ($\pm 4.1\%$) of people use 2FA.** That figure proved to be a lot lower than we expected, but it makes more sense when considering the responses to our follow-up questions concerning use and knowledge of 2FA.
- Over half of the study participants ($56.43 \pm 4.6\%$) **had not heard of 2FA** prior to our survey.
- There were also 8 participants (1.8%) who indicated that they **had used 2FA but no longer use it**.
- When asked what their primary reason for no longer using 2FA, seven of the eight participants cited inconvenience as the driving factor.

Who is Most Likely to Use 2FA?

Let's dig into that 28% (126 participants) a little more. To compare people of different demographics, we used the **Pearson χ^2 test**. During our analysis, we noticed that the use of 2FA was not independent of age ($X^2 = 31.09$, $p = 8.98e-06$), gender ($X^2 = 6.68$, $p = .009$), and employment status ($X^2 = 47.41$, $p = 4.70e-09$).

In regards to age, the older individuals were less likely to be using 2FA. When it came to employment status, individuals who were a student or employed were more likely to use 2FA. And finally, men were more likely to use 2FA than women.

Why Did People Start Using 2FA?



We were also interested in what prompted users' adoption of 2FA. Surprisingly, over half (54%) of participants implemented it voluntarily. This was a much higher percentage than we could have estimated. We anticipated a similar percentage from our 'involuntary' option since we assumed most people began using 2FA because of their employer. However, this may come from the fact that only 20.8% of people learned about 2FA from their workplace.

Where Do They Use 2FA?

In addition, we asked those same 126 participants whether or not they use 2FA on all of the websites and/or apps that offer it or just some of them. Forty-five percent of those respondents reported said that they used 2FA on all the services that offer it. That figure proved to be higher than our initial estimates.

In many cases, survey respondents will answer with the most socially acceptable or "correct" answer. They may also be unaware of the option to enable 2FA with other services. It is impossible to know if that is truly the case here, but we can speculate.

Last, we asked those who use 2FA for only some of their 2FA-supporting services (55% of all 2FA users) about their motivation for that behavior. The two most prevalent answers were "Those services for which I enable 2FA are more important to me and hold data that I want to protect" (42.03%) and "I am required to use 2FA for those services" (49.28%).

Adoption of Different 2FA Methods and Technologies

As we mentioned earlier, our study was an update to the comparative usability study that was conducted in 2010. A lot has changed since then. Two-factor authentication involving push notifications or simple app interactions did not exist, and neither did security keys. We asked participants which methods and/or technologies they had used as well as a series of questions about their usage experiences.

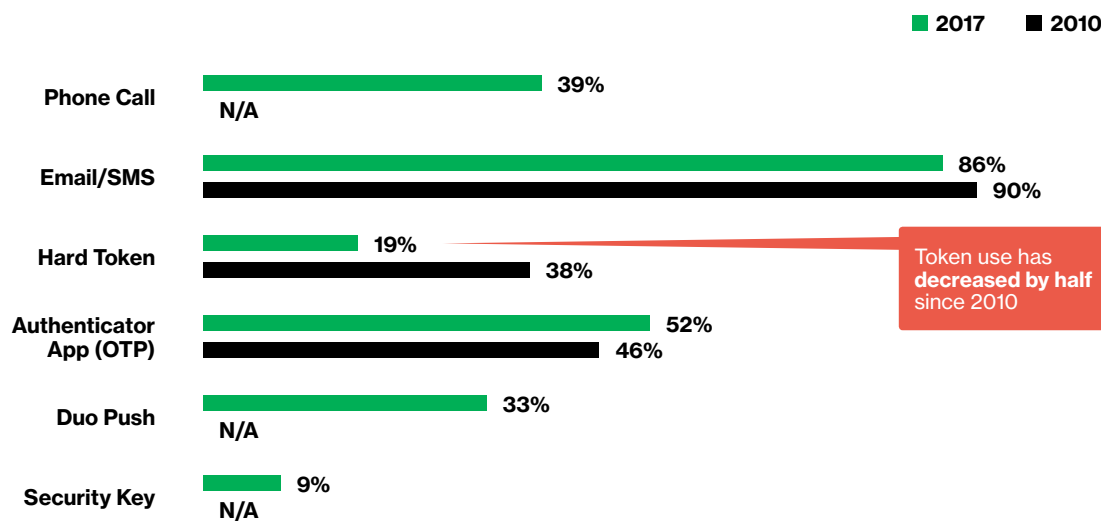
As you can see in the table below, 2FA via email or SMS (85.82%) was the most popular. That's not particularly surprising because many websites and applications that offer 2FA had SMS as the default option, plus it as well as phone call been around the longest. If we were to conduct this study next year or a few years from now, it would be interesting to see if this figure changes.

With the information out there about the ease of social engineering wireless carriers to forward messages to another SIM card or intercepting messages through fake cell towers, we hope that any change in that percentage is in the downward direction. Further discussion about the National Institute of Standards and Technology's (NIST) response to this information can be found in the Context of Use section.

The method with the least adoption (8.96%) was 2FA via security key. This was expected since U2F tokens/ security keys are the youngest of the 2FA technologies and requires the user to procure an additional device.

However, we were surprised by the result itself. 8.96% is more than 1 in every 12 people that use security keys, or at least claim to. In regard to changes over time, more people have had experience using authenticator apps (5.37%) than they did in 2010. With more usable methods being available, there has been a decrease in the use of hard tokens (18.70%) as well.

2FA Usage by Method



Perception of Different Methods and Technologies

In order to better understand how the survey participants experienced using each of the 2FA methods, we used Likert items similar to the Likert scale questions in the **System Usability Scale (SUS) questionnaire**. In the table below, we list the 2FA methods that people most agreed with (Strongly Agree, Agree, or Somewhat Agree) and the technology that people least agreed with in regards to the statements that were asked.

One of the more surprising findings was that people found hard tokens most trustworthy (84%). On the other hand, they also were least likely to agree that hard tokens were more secure than email and passwords. Since we didn't ask participants follow-up questions, we can only speculate on why this is the case. One possible cause would be concern over network connectivity on phones, while a hard token is always on and wherever you left it. Users may **trust** the hard tokens to work all the time, while still not having confidence in the security of those 6–8 digits.

We have plenty of anecdotal evidence regarding the experience when people use **Duo Push** and the data in our survey corroborates that. When it came to frustration, concentration needed, and requiring instructions to use it, 2FA via push notifications scored the best.

Question	Most (highest percentage that agree)	Least (lowest percentage that agree)
I thought it was convenient	Security Key and Push Notification (66.67%)	Authenticator App (52.89%)
Using it was quick	Security Key and Push Notification (66.67%)	Hard Token (32%)
I enjoyed using it	Security Key (58.33%)	Hard Token (40%)
I would be happy to use it again	Push Notification (63.44%)	Phone Call (51.92%)
I found it user friendly	Security Key (75%)	Hard Token(44%)
Found it trustworthy	Hard Token (84%)	Phone Call (51.92%)
Felt it was more secure than using just username and password.	Security Key (66.7%)	Phone Call (50%)
I needed instructions to use it.	Security Key (33.33%)	Push Notification (13.33%)
I had to concentrate while when using it	Hard Token (44%)	Push Notification (20%)
Using it was stressful	Security Key (25%)	Phone Call (5.77%)
Using it was frustrating	Security Key (41.67%)	Push Notification (4.44%)

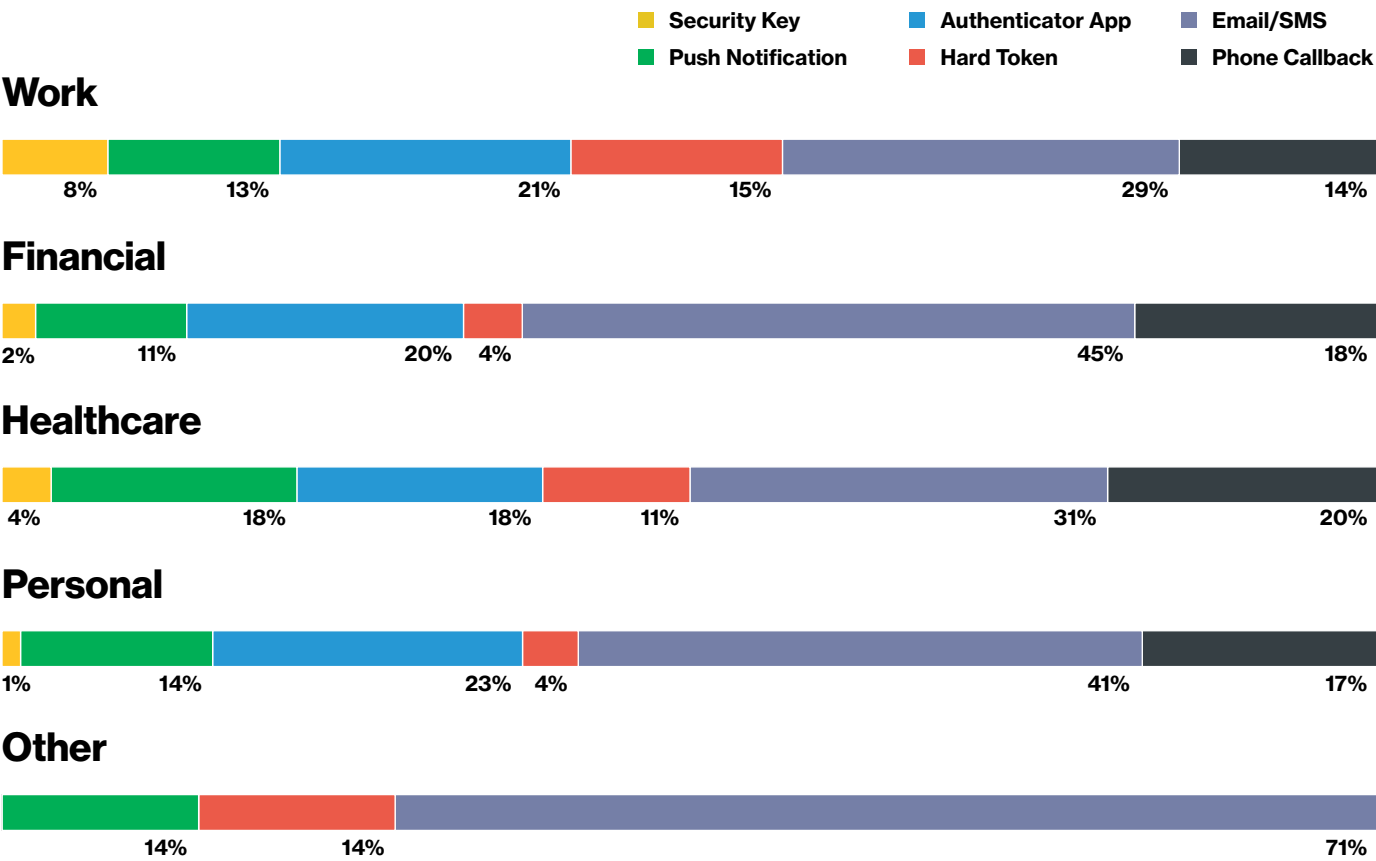
Context of Use

In addition to understanding which technologies people have used and their experience using them, we also wanted to understand in which contexts they used them. With email/SMS being the most popular 2FA technology, we expected it to make up the highest percentage of use in each of the contexts, and it did. While that isn't surprising, it does create some pause.

Last July, **NIST acknowledged** the general insecurity of out-of-band authentication via SMS due to its susceptibility to interception or redirection. Moreover, in the most recent revisions to the **Digital Identity Guidelines**, they have acknowledged that methods like voice-over-IP (VoIP) or email do not prove the possession of a specific device. Since our question concerning SMS only asked, "In which of the following context(s) have you used email/SMS as your second factor?" we have no way of determining its prevalence in each of the contexts we asked about.

Outside of SMS, the difference in use of security keys outside of the workplace was also something of note. We believe that this shows that the people charged with securing their organization's environment understand the security properties that are guaranteed by security keys and thus make them available in the office; however, it seems as if that same knowledge has not made its way to the general populous or that authenticator apps are deemed sufficient.

2FA Methods by Context



Conclusion

This survey underscores the reality that we as a security community still have a long way to go when it comes to educating the everyday person about proper security behaviors in general and 2FA in particular. We believe the crux of that disconnect is that most people don't understand the importance of 2FA in helping prevent unauthorized access.

Similar to advice concerning physical hygiene and wellness, security hygiene can often be overlooked and the consequences of not following are not understood until a harmful event occurs. Fear should not be used as a means of encouraging users to adopt certain habits or behaviors, but pointing to examples where 2FA would have helped prevent particular incidents could help users better understand why they should use it.

For those that do use 2FA, we also need to educate them that all 2FA methods are not created equal. Keeping with our physical hygiene analogy, this could be the difference between a conventional toothbrush and one that is electric. Brushing your teeth with a conventional toothbrush is better than not brushing all; however, an electric toothbrush is better. Similarly, using SMS is better than nothing but it isn't as good as an authenticator app which isn't as good as using a security key.

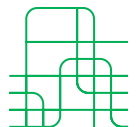
Approaching this issue is distinctively more difficult because it involves helping users understand the security properties of each method. With that being said, it will continue to be important for security practitioners and engineers to understand the mental model of the general populous as it relates to 2FA.

Looking Forward

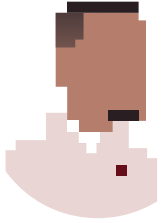
This report only examines data from the survey we conducted. We hope to add to these findings by gaining a greater understanding of when 2FA started being offered at popular sites, as well as what types of factors they offer, because the ecosystem looks very different if everybody is using only SMS, instead of seeing deployment of more secure methods, like U2F.

Another question of interest is how users actually use 2FA. Do users that initially use SMS change to more secure factors on their own? What if unobtrusive user education is provided? How much does their actual behavior align with their impression of their behavior, as reported from this survey?

We learned a lot by conducting a survey of this size and hope that we can continue doing projects like these to gain a greater sense of the security behaviors of non-expert users. We won't ever fully educate all users, so understanding their instincts and perceptions is critical to building security features that empower the user to make the right decisions.



About the Authors



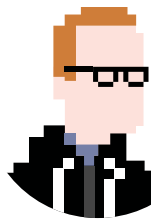
Olabode Anise

[@justsayo](#)

Data Scientist

Olabode is a Data Scientist at Duo Security where he wrangles data, prototypes data-related features, and makes pretty graphs to support engineering, product management, and marketing efforts.

Prior to working at Duo, Olabode studied usable security at the University of Florida. When he's not at work, he spends his time exploring data-involving topics such as sports analytics, relative wages and cost of living across the United States.



Kyle Lady

[@kylelady](#)

Senior R&D Engineer

Kyle is a Senior R&D engineer at Duo, where he harasses everyone for more data to try to satisfy the unquenchable thirst for analytics that academic research imparts. He has broken the Internet only once.

Kyle studied computer science at the University of Michigan.



Our mission is to protect your mission.

Experience advanced two-factor authentication, endpoint visibility, custom user policies & more with your free 30 day trial.

Try it today at duo.com.

Duo Security makes security painless, so you can focus on what's important. Our scalable, cloud-based **Trusted Access** platform addresses security threats before they become a problem, by verifying the identity of your users and the health of their devices before they connect to the applications you want them to access.

Thousands of organizations worldwide use Duo, including Facebook, Toyota, Panasonic and MIT. Duo is backed by Google Ventures, True Ventures, Radar Partners, Redpoint Ventures and Benchmark. We're located from coast to coast and across the sea.

Follow [@duosec](https://twitter.com/duosec) and [@duo_labs](https://twitter.com/duo_labs) on Twitter.



**The Trusted Access
Company**

duo.com

