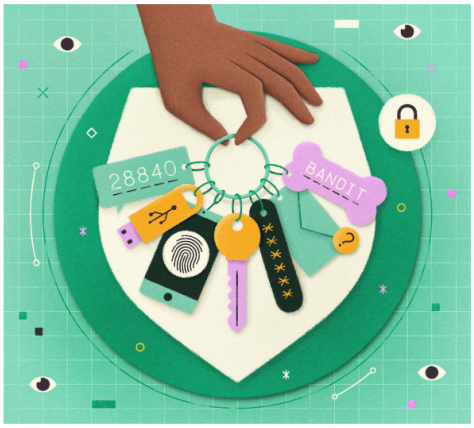
MFA

How to Use Psychology to Increase MFA Adoption

Common cognitive biases may be impacting your MFA adoption rates; here are some ways to counter those impacts.




Nabeel Saeed
Product Marketing

June 09, 2021

TABLE OF CONTENTS

Multi-factor Authentication (MFA) has been shown capable of blocking up to 99.9% of brute force attacks. Yet a recent IBM/Ponemon Institute study found that only 36% of responding organizations require it. And adoption numbers for the general public aren't encouraging either, with a report from LastPass finding that only 37% of respondents use MFA for their work accounts. When you add the finding by Verizon that 80% of data breaches involves the use of stolen credentials, these numbers beg the question, why?

If MFA has been proven so effective as a defense against data theft and brute force attacks, why are adoption numbers still so low? A common set of issues revolve around what are called cognitive biases. We're going to look at some of the most common cognitive biases, why they're so effective at keeping adoption of new security measures down, and how you can turn the tables and work with these same psychological ideas to counter their impact and potentially increase MFA adoption.

Cognitive Bias Overview

Before we dive in and look at the ins and outs of cognitive biases, it would be helpful to ensure we're all on the same page about just what is meant by that phrase. A cognitive bias is a subjective reality that we all create for ourselves, most often based on available information and our own life experiences.

Cognitive biases are often the result of using heuristics, a type of mental shortcut or rule of thumb, to speed decision making amidst uncertainty. People walking through the steps of creating a new account, for example, will know, based on experience, if the process seems to contain too many, or too few, actions. If they don't find what they expect, they may abandon the process in favor of one that feels like it has a better mix of ease-of-use and security.

With all of that in mind, we turn to a sampling of the cognitive biases that may be impacting the adoption of security features like MFA. We will also address how each cognitive bias has a flip side or a way to approach it that can flip its effect from detrimental to beneficial for your adoption rates. A quick note: more information on each bias/heuristic discussed here can be found on Decision Lab's list of cognitive biases.

1. Optimism Bias

What it is — People tend to overestimate the chances of positive events while simultaneously underestimating the chances of negative ones. This has the result of giving us a feeling of control over situations where, in fact, we may have little to no control.

How it can impact adoption — The basic argument looks like this: "data theft happens to other people; it will never happen to me." Therefore, people who feel this way don't see the point in adopting additional security measures such as MFA, especially if doing so feels at all invasive or time-consuming. This feeling was verified in a recent report from cybersecurity company Balbix which found that 99% of enterprise users reuse their passwords, either across work accounts or between corporate and private logins.

How to work with it — The underlying shortcut being used here says that since something has never happened before, it won't happen now. Remember that you're asking people to take steps to protect themselves and your organization. You can use their optimism in your favor by offering an incentive for adoption. For example, the online game Fortnite offered a free victory dance emote for everyone who opted into their new MFA feature. Other companies like Google are deciding to require users to enable MFA. For most companies, this strong-arm tactic may not be the best route to take for customer satisfaction, especially when you can work with these psychological ideas to achieve the same goal while maintaining a great CX.

2. Fundamental Attribution Error

What it is — The habit of attributing dispositional factors, rather than situational ones, for other people's behavior. For example, when someone cuts you off in traffic, our instinct is to assume they're just a bad person, instead of taking into account the possibility of their being late for an interview or on the way to the hospital because a loved one was injured.

How it can impact adoption — People will think, "I don't need the extra security because I'm not like those other people who don't know how to create good passwords." This thinking combines the fundamental attribution error with its opposite, the actor-observer bias, which states that we overemphasize situational factors to our own behavior over dispositional ones.

How to work with it — Use the actor-observer effect to your advantage by showing customers how quick and easy it is to set up and use MFA. This eliminates the primary situational excuse of "I'm too busy." Adaptive MFA allows you to only confront your customer with additional verification steps when the situation calls for it. At the same time, variable options for that authorization keep the additional step as low-friction as possible. For example, using the biometric features of the visitor's smartphone is an extremely secure and low-friction second verification method that users already trust.

3. Status Quo Bias (Psychological Inertia Effect)

What it is — A basic preference for the current state of affairs. Psychological inertia further describes our reluctance to make changes to the systems we see as working just fine, despite the appearance of disconfirming evidence.

How it impacts adoption — Thinking that "how I do it has worked for years, why should I change now?" can lead to things like reused passwords and a general lack of willingness to adopt new processes despite the mounting evidence that factors like MFA are key to slowing down or stopping data theft.

How to work with it — The need to maintain control is often at the root of status quo bias. That means that a gentle reframing of the ask (enable this new feature) may be called for. Wording like "keep control of your account with MFA" can be enough to sway users who are on the fence. Point out that with adaptive MFA, the user won't even see the additional step on every login, only in situations where a special circumstance is detected. Circumstances like impossible travel, where a login attempt makes it look like the user has traveled farther than possible in the time since their last login, for example.

4. The Framing Effect

What it is — Choices can be presented in ways that highlight positive and/or negative aspects of the decision being made. The context in which the options are presented can make the difference in how the decision-maker feels and which option they ultimately choose.

How it can impact adoption — If MFA looks like an extra step in what is already viewed as an overly complicated process that you're imposing on your audience, they're less likely to be willing to adopt it.

How to work with it — Most of us frame our decision-making based on availability and affect (how we feel in the moment). If you can slow down the process just enough for people to realize the importance of the decision, they're more likely to take more aspects into consideration and will therefore be more willing to take the extra moment or two to set up added security for the peace of mind it will give them down the road. Reframing the decision as being about maintaining control over your personal information by removing mention of the organization or data breaches overall can also help here. Another step you can take is to leverage Auth0 features like Breached Password Protection (BPP). With this enabled, users will be notified should their credentials be found in a data leak; you can use that to encourage adoption of MFA to block a possible attack on their information. Now they know you're watching out for them, making them more receptive to doing their part by enabling MFA protection.

5. Dunning-Kruger Effect

What it is — This bias states that people with limited knowledge of a topic tend to overestimate their ability in that area. This effect is often misinterpreted as saying something about the intelligence of people in general, which is unfortunate because that means it's often used incorrectly. In our scenario, this effect will most often look like someone saying, "my password is uncrackable," or "I'm smarter than some criminal."

How it impacts adoption — Once someone is overconfident in their ability to maintain security over their information, they are not likely to think they need what they now view as unnecessary added steps. The thinking is that since they're so much smarter than criminals and have created an uncrackable password, why should they bother setting up additional protection?

How to work with it — Slow down and make MFA the default. David Dunning, one of the psychologists credited with the effect's discovery, has this to say, "The first rule of the Dunning-Kruger club is you don't know you're a member of the Dunning-Kruger club." In essence, we all suffer from this bias at some point and likely have no idea that it's happening. The way to combat this is to add just enough friction to the account creation process that people take the time to realize the importance of MFA. Add to that making MFA an opt-out feature, rather than opt-in, so it becomes faster and easier to leave the default setting and enable it.

Cognitive Biases Need To Be Accounted For

Keeping in mind the possible cognitive biases at play allows you to design customer experiences (CX) that encourage your audience to make safer decisions. Paying special attention to your CX, along with the content and specific wording used, can go a long way toward increasing customer adoption of MFA. By using framing to encourage adoption, remembering to keep things positive, and showing how MFA use enables the user to maintain control over their own personal information — you're setting yourself up for better adoption rates.

Auth0 provides the flexibility to A/B test different CX designs and content so you can find the right way to frame the decision for your audience. And the scalability we offer means that as more users opt-in, the infrastructure will be there to support your growing user base. Adaptive MFA will also play a large role in the success of your MFA adoption efforts. With features like Bot Detection, impossible travel, and IP reputation scoring, your users will only be presented with the MFA window when the situation warrants it. When you're ready to learn more about how Auth0 can help you create a CX environment that fosters better MFA adoption, start with our MFA Guide blog post, then reach out to our experts to start the conversation.

About Auth0

Auth0 by Okta takes a modern approach to customer identity and enables organizations to provide secure access to any application, for any user. Auth0 is a highly customizable platform that is as simple as development teams want, and as flexible as they need. Safeguarding billions of login transactions each month, Auth0 delivers convenience, privacy, and security so customers can focus on innovation. For more information, visit https://auth0.com.

Nabeel Saeed

PRODUCT MARKETING

Nabeel is a product marketer focused on all things security and identity. He has contributed to publications like Wirecutter, Information Age, and Professional Security. He has also been a guest speaker at the Bay Area Cybersecurity Meetup, and delivered talks on IAM across the US, Canada, Israel, and Singapore. He is passionate about helping build secure auth experiences that amaze users and delight businesses.

VIEW PROFILE

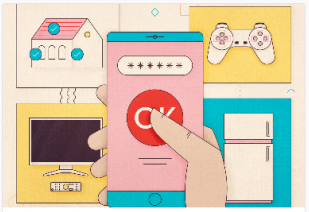
More like this

ADAPTIVE MFA

Auth0 Introduces Adaptive MFA

MFA

MFA With WebAuthn for FIDO Device Biometrics Now Available



AUTHENTICATION

Enable SMS MFA Using Any Provider

Follow the conversation

Powered by the Auth0 Community. Sign up now to join the discussion. **Community links will open in a new window.**

1 reply

robertino.calcaterra Auth0 Employee ↩ Reply to comment

Let us know if you have any comments or thoughts!

CONTINUE DISCUSSION

Auth0 by Okta | Community

Secure access for everyone. But not just anyone.

TRY AUTH0 FOR FREE

TALK TO SALES