# Is Duo Authentication Safe?

**If you're looking to implement a multi-factor authentication (MFA) solution, Duo MFA has probably crossed your mind as an option. But is it the safest choice on the market? Not by a long shot.**

**Learn more why Duo MFA with its push notifications, one-time codes, and passwords is vulnerable to attacks.**

## Duo MFA still uses passwords

Passwords can and will be hacked and Duo does not totally eliminate passwords from the authentication process and recovery. So even with Duo MFA enabled, you're still at risk of password-based hacks, which are responsible for 85% of all cyberattacks.

## Duo MFA uses phishable factors

In addition to passwords, the Duo MFA platform uses factors that attackers can phish. The default authentication method is Duo Push, which are push notifications to a registered mobile device. Depending on how an organization sets up Duo, other phishable methods like time-based one-time passcodes, passcodes sent through SMS text messages, or phone callbacks can be used.

Cybercriminals are able to surpass these weak, phishable factors with ease, and it's one of the reasons the US government is mandating that federal agencies move away from these hackable factors and onto phishing-resistant MFA.

## Duo's need for a second device creates UX friction, which hurts adoption

MFA can be a friction-filled authentication experience, which hurts adoption rates. Microsoft reported that only 22% of Azure Active Directory users have MFA in place, with user experience presumed to be the main barrier to adoption.

Duo's MFA is no different. Users need to have their second device on hand and be ready to enter in a code or get a push notification in time. If they forget their password, there's still cumbersome password resets and policies that users need to follow. Frustrated users look for workarounds, and any protection that was in place is totally negated.

## Beyond Identity provides phishing-resistant, passwordless MFA

Beyond Identity's passwordless MFA only uses secure, phishing-resistant factors that provide true protection against cyber threats. Instead of using passwords paired with other phishable authentication factors, Beyond Identity only uses:

- **Local biometrics:** Using biometrics allows for a frictionless user experience, while also providing more security than a push notification or SMS text message.
- **Cryptographic security keys:** This "something you have factor" makes sure that a user is only allowed to login from a trusted and authorized device.
- **Device-level security checks:** Beyond Identity checks what data and resources the device in question is trying to access and checks the device's security posture to make sure that insecure devices are stopped cold.

Beyond Identity is not new to passwordless and this technology has been baked into our product since day one. We've had a market-ready solution that lets organizations ditch the password once and for all and all the costs associated with them. We also integrate with the most popular SSOs and it is as easy as adding a few lines of code to get your workforce up and running.

Everything, from authentication, customizable risk policies, and admin controls are all centrally located in a single platform. Every one of our customers receives individualized support and a central point of contact to ensure deploying Beyond Identity is as smooth as possible.

We'd love to show you why Beyond Identity is the safer MFA solution. Ask for a free demo today.

### Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in–eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.