



Passkey Index

October 2026

www.fidoalliance.org



Executive summary

Passkeys have moved from deployment to adoption. While last year's Index showed that passkeys were available to almost every user, the Passkey Index 2026 shows they are being routinely used. **More than one in three successful sign-ins now use a passkey (36%),** up from roughly one in four in 2025 (26%). Enrollment has grown too, but more slowly; the bigger change is that people who have a passkey are now using it more of the time.

The benefits of passkeys are also clearly established in the Index. Passkey sign-ins succeed more often than traditional MFA sign-ins (**93% vs 78%**) and are **nearly three times faster** than signing in without one, saving users an average of **27 seconds** per sign-in. **Every participant that measures phishing** has reported fewer successful attacks since deploying passkeys, and every participant that provided savings data reported lower SMS OTP costs.

The next step is making passkeys the default. While the gap is closing, most participants still see more users enrolled than signing in with a passkey. However, two-thirds plan to offer passwordless accounts in the next 12 months, which we expect to both drive passkey adoption and remove less secure and less effective alternatives and fallbacks.

Overview and methodology

The 2026 Passkey Index draws on data and insights provided by 15 consumer relying parties from across the globe. Submissions were confidential and no figure is attributed to any organization. Results were compiled on 21 September 2026. Percentages, times and ratios are unweighted averages across the participants that reported them. Not every participant answered every question, so each figure notes how many contributed (n).

Comparison with 2025. This year's Index has 15 participants, compared with 9 in 2025. Comparisons with last year are therefore directional: they show how this year's group compares with last year's, not change within the same group of organizations. Comparisons are made only where the metric was measured the same way in both years.

Changes to the questionnaire. Two questions are new this year: whether successful phishing attacks have decreased since deploying passkeys, and whether the organization plans to implement passwordless accounts in the next 12 months.

Case examples. Alongside the aggregated findings, participants submitted individual results and observations that cannot be averaged, because they use different metrics, currencies or periods, or come from a single organization. A selection appears in “Passkeys in practice”. Each is one participant's own figure, unattributed, and cannot be linked to any other example or to the aggregated findings.

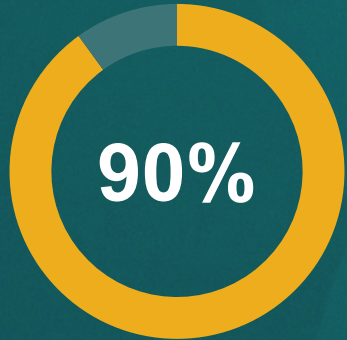
15 consumer relying parties
compared with 9 in 2025

Abanca	Mercari
Amazon	Microsoft
BanESCO	NTT DOCOMO
CVS	PayPal
Google	Shopify
JP Morgan Chase	TikTok
KDDI	WhatsApp
LY Corporation	

Results compiled 21 September 2026

Finding 1

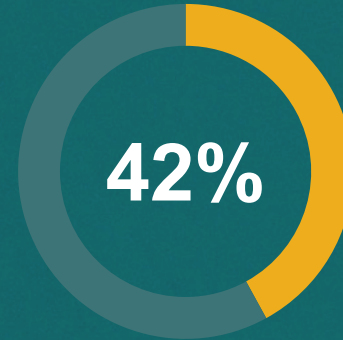
Passkeys are within reach for almost every user



of active accounts are eligible for passkeys

7 of 13 participants offer passkeys to their entire account base.

n=13



of eligible accounts have a passkey enrolled

Roughly 38% of all active accounts.

n=13

Where eligibility is below 100%, participants describe it as a deliberate scoping choice, such as channel sequencing or device-quality gating, not a technical limit.

Index insight: Last year's Index reported 93% eligibility and 36% of eligible accounts enrolled. Eligibility is slightly lower this year, consistent with a broader mix of sectors and regions; enrollment is up 6 percentage points.

Finding 2

Passkeys are becoming a routine way to sign in



Index insight: Last year's Index reported 26%, an increase of 10 percentage points in 2026. Sign-in share has grown faster than enrollment (up 6 points), so more of the people who have a passkey are using it.

Sign-in share includes re-authentication and excludes account recovery. It covers participants that offer passkeys as a sign-in method.

Finding 3

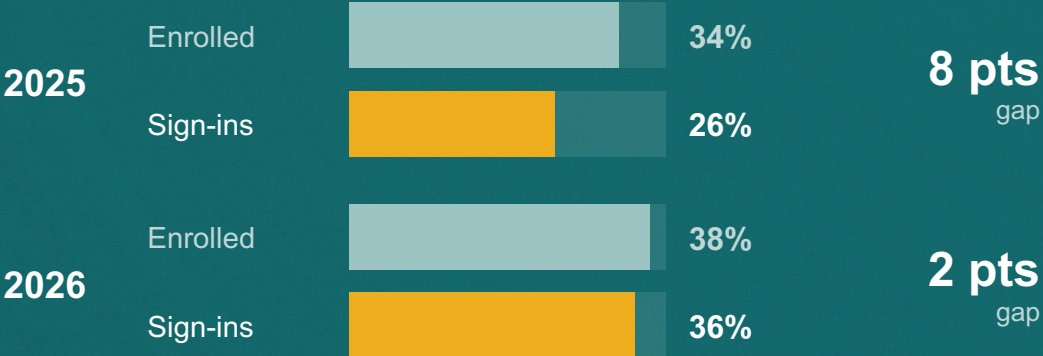
The gap between having a passkey and using it is narrowing

Among participants that report both enrollment and sign-in share



still have a passkey sign-in share below their enrollment rate: users have a passkey but are not always routed to it, or able to use it, at sign-in.

The gap is narrowing



Enrolled = share of all accounts with a passkey. Sign-ins = share of successful sign-ins using a passkey.

Index insight: In 2025, 34% of all accounts had a passkey but only 26% of sign-ins used one, a gap of around 8 percentage points. This year it is 38% against 36%, a gap of around 2 points. Making the passkey the default path for users who have one is where the next gains in share will come from, and Finding 6 shows most participants intend to do exactly that.

Finding 4

Passkeys outperform other sign-in methods on success and speed

Sign-in success rate

Passkeys



Passwords and traditional MFA

93%

78%

+15

percentage points higher success with passkeys

than passwords and traditional MFA such as SMS OTP and authenticator apps (n=12)



2.8×

faster sign-in with passkeys than without

All 9 participants that measured speed report faster sign-in (n=9)



27 sec

saved per sign-in on average

Indicative figure, based on each participant's own time difference (n=9)

Index insight: The advantage is near-unanimous: passkeys delivered faster sign-in for every participant that measured speed and higher success for 11 of 12, which means fewer failed attempts and less friction at the sign-in, checkout and payment steps where drop-off costs the most.

Finding 5

Successful phishing attacks are falling after passkey deployment



of participants that measure it report a decrease in successful phishing attacks since deploying passkeys



8 of 8 participants that measure it. New question in 2026.

Index insight: Phishing resistance is the core security argument for passkeys. This is the first time the Index has evidence of that benefit from production deployments, and it is unanimous.

Finding 6

Going passwordless is high on next year's agenda

9 of 13

participants that answered plan to implement passwordless accounts in the next 12 months



- Planning in the next 12 months (one on an exploratory basis)
- Researching it
- No plans in that period

9

plan to implement passwordless accounts in the next 12 months

1

is researching it

3

do not plan to in that period

Index insight: Passwordless accounts can eliminate the fallback that keeps enrolled users on passwords and are one of the clearest opportunities to close the gap between enrollment and use described in Finding 3.

Passkeys in practice

Participants also provided individual examples and data. Each describes one organization's experience, offered as insight into how passkeys play out in practice, not as a measure of how common that experience is. Examples are not aggregated or attributed.



SMS OTP costs fall

All four participants that provided savings figures report reductions, with the actual saving depending on each participant's context. Reported annual savings ranged from approximately \$1 million to hundreds of millions of dollars, reflecting differences in organization size, passkey adoption and SMS usage.



Account takeovers fall

Three participants shared observations on account takeovers, all reporting fewer since deploying passkeys, with one seeing 'virtually none' among users who sign in with a passkey.



Sign-in flows should favor passkeys

Two participants say their sign-in flow shows a password or OTP before offering the passkey, even to users who have one. One of them estimates that offering the passkey first would roughly double its passkey sign-in share.

What comes next

The 2026 Index shows passkeys have moved beyond availability and into everyday use. More users are enrolling, more sign-ins are happening with passkeys and organizations are seeing measurable benefits in sign-in success, speed, security and cost. This builds on top of the 2025 Index, that showed that passkeys were being deployed and adopted at scale, with benefits in conversion rate, time to sign in and decreased costs.

The next phase is about making passkeys the default, moving from offering passkeys as an option to building experiences around them. Continuing to increase enrollments, while removing weaker forms of fallback such as passwords and SMS, will ensure a great user experience with the highest level of security. The data shows that organizations are planning to deploy passwordless accounts to address that.

The Passkey Index will continue to track this evolution: how quickly enrollment and usage grow, whether passwordless plans become real-world deployments, and how the security, business and user experience of passkeys develop as adoption matures.



www.fidoalliance.org

www.passkeycentral.org

