1Password

REPORT

Preparing for a passwordless future

Passwords are reaching their limit.
Passkeys are a better way.

Executive summary

Passwords are difficult to remember, annoying to input, frustrating to constantly change – and, as news headlines highlight on a daily basis, they're all too hackable.

As online service providers seek to boost cybersecurity by requiring multi-step login processes and increasingly complex passwords that incorporate a dizzying mix of letters, numbers, and symbols, logging in is becoming even more of a burden. It's also becoming a more frequent necessity, as people access an avalanche of websites, apps, and accounts while juggling multiple devices.

Fortunately, there's a better way.

Passwordless technology – which aims to relegate passwords to a thing of the past – is poised to transform our online lives, by making logging in much easier to navigate and far more secure. If we eliminate passwords, we also eliminate the login friction and frustrations that many of us have grudgingly accepted as unavoidable facts of digital life. We also virtually eradicate the risks of phishing attacks – in which scammers send messages that appear to come from a trusted person or entity, but are really meant to trick users into divulging sensitive information. Simply put, if there's no password to steal, there's nothing to phish.

To better understand consumers' receptivity to passwordless technology, 1Password surveyed 2,000 North American adults on their attitudes about passwords. The survey asked about their familiarity with passwordless logins, including passkeys – which are the most promising and secure alternative to passwords, with growing support from major platforms like Apple, Google, and Microsoft. The survey also asked about respondents' openness to adopting passwordless options and the priorities that determine their willingness to experiment with emerging technologies in general.

Our findings reveal that nearly two in three people (65%) are open to using any new technology that makes their lives simpler, while half (50%) actively want to adopt new life-simplifying solutions. While most people aren't yet familiar with passwordless technology, our survey shows that consumers are ready to give it a try – especially those who already access accounts or devices using a fingerprint, facial recognition, or other types of biometrics.

For passwordless technology to go mainstream, consumers need to understand not only how this novel way of logging in can simplify life, but also how it works and that it's secure. Knowledge is crucial. In fact, 34% of people say they regret adopting certain technologies before they fully understood them. Among survey respondents, 43% say they want to start using a new technology only after understanding how it functions, while 38% want assurance that it's safe and secure.

It's not enough for passwordless technology to be simple and secure. Widespread adoption will require that consumers and businesses alike trust and understand that it's simple and secure. A passwordless future holds great promise – and consumer education can pave the way.

Key findings

FED UP WITH PASSWORDS

Seeking simplicity

Nearly two in three people (65%) say they're open to using any new technology that makes life simpler.

Login exhaustion

Seven in 10 people (70%) say having to remember or reset their passwords is a regular annoyance.

Safety first

77% of people would love a more secure way to log in to accounts.

Pervasive phishing

67% of respondents personally received phishing attack messages in the past year, while **100%** either received phishing messages or know someone who did.

Fake friends

People say they're most susceptible to phishing attacks purporting to come from their bank **(43%)**, a friend **(41%)**, or their spouse **(39%). Just 25%** say they're likely to fall for a phishing message that looks like it's coming from their boss.

INTRIGUED BY PASSWORDLESS

Pushing past passwords

Only a quarter of people (25%) have heard of "passwordless," but **more than half (58%)** are open to using something other than a password to log in to their accounts.

Preference for passkeys

Three in four people (75%) indicate they'd consider using passkeys, while **nearly one in five (19%)** say they'd start using passkeys as soon as they're available.

Biometrics boom

87% of those already using biometrics are open to using passkeys, compared to **57% of those not using biometrics.**

Look before you leap

43% of people are motivated to try a new technology when they understand how it works, while **38%** say they need assurance that it's safe and secure.

Work and retail are key

81% of people are at least somewhat open to logging in to work accounts using a method that doesn't involve a password, while **77%** are at least somewhat open to accessing retail accounts in this way.

01

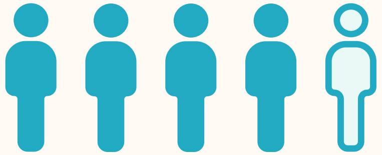
The password predicament

As the number of websites, apps, and accounts people log in to daily continues to rise, the volume of passwords we must manage and memorize grows, too.

Consumers care deeply about their online privacy and security. But it’s frustrating to go through the rigamarole of constantly creating and resetting increasingly complicated passwords for every account – and the reality is, we're not very good at it. Previous 1Password research has found that 51% of people store their passwords by memory and that 34% of employees reuse passwords despite knowing the risk.

The evidence is clear: We need a better way.

PASSWORDS' TIME HAS PASSED



Four in five people (80%) say they care about their online privacy and actively take measures to protect it. But in a world that prizes innovation and user experience, the process of logging in with a password is stuck in the past.

70%

say that having to remember or reset their passwords is a regular annoyance.

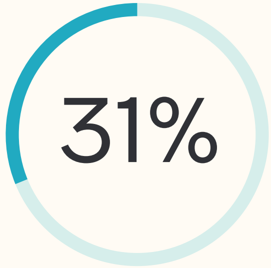
77%

would love a more secure way to log in to accounts.

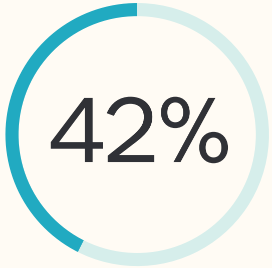
BELEAUGUERED BY BREACHES

Damaging security breaches regularly disrupt large corporations that many of us do business with, generating a steady stream of headlines. According to Verizon's 2022 Data Breach Investigations Report, 82% of breaches involve a human element – meaning that a person has made an error, had their credentials stolen, or otherwise introduced a critical vulnerability. Our own data reflects that people are worried about data leaks, hacks, and cyberwarefare – and that many realize they've made security mistakes.

Nine in 10 people are worried about a data breach.



Nearly one in three people have already experienced a data breach.



Four in 10 people have a digital-security-related regret about using technology, such as wishing they'd created better passwords or responded differently after a breach.

SIMPLE AND SAFE

Modern life is overwhelming, and people look to technology to simplify things.

But when it comes to cybersecurity, some worry that simple and secure are contradictory – and inaccurately believe that when logging in requires more legwork, it's safer.

25% of people mistakenly believe that if digital accounts are easy to access, they're less secure.

65% of people say they're open to using any new technology that makes life simpler.

85% of people say they want security technology and features to be as simple as possible to use.

02

The word on passwordless

Passwordless. It's an intriguing term for technology designed to transform how we engage with the online world. While the concept is gaining traction, our research found that many consumers are still confused about what passwordless is and the differences between varying types of passwordless logins, including magic links, physical security keys, and passkeys.

THE WORD ON PASSWORDLESS

Here's more context for the concept as a whole and the most promising form of passwordless technology: passkeys.

Passwordless, defined

Passwordless refers to any form of technology or process that lets you access an account or online service without relying on a password. Because passwords are the source of breaches, passwordless has the potential to reshape our online interactions by making logging in to apps and services simpler and far more secure. It's important to note that not all forms of passwordless technology are created equal.

Passkeys, defined

Passkeys, which replace passwords entirely, are the newest and most secure form of passwordless technology. Every passkey consists of two interlocking parts: a public key that's shared with the website or app you're creating an account for, and a private key that never leaves your devices. Both are needed to authenticate you, and it's impossible to reverse-engineer one key from the other. Without physical access to your devices (and a way to unlock them), no one can log in to your passkey-protected accounts. Consider the public key like a magic ink pen and the private key like a special light required to read the secret message. Even if someone gets hold of the pen, they can't read the message without the light.

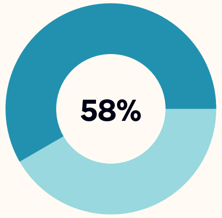
Passkeys are incredibly easy to use, extremely secure (there's no such thing as a weak passkey), and championed by every major platform. When you unlock your device with biometrics such as facial recognition or a fingerprint – and then access your accounts using passkeys – this creates an entirely passwordless login experience, from start to finish.

PASSWORDLESS PROMISE

While the term “passwordless” has yet to go mainstream, it’s making its way into our collective consciousness – even earning attention from late tech adopters.

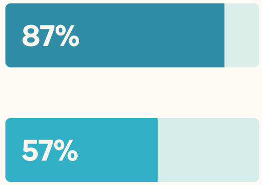
One in four people (25%) say they’ve heard the term “passwordless.”

BIOMETRICS BOOM



More than half of people (58%) already use biometric logins, whereby they access devices such as phones and computers with a fingerprint or facial recognition.

Familiarity with biometrics has a strong correlation with openness to passkeys – suggesting that as biometrics become even more popular, people will be more receptive to using passkeys.



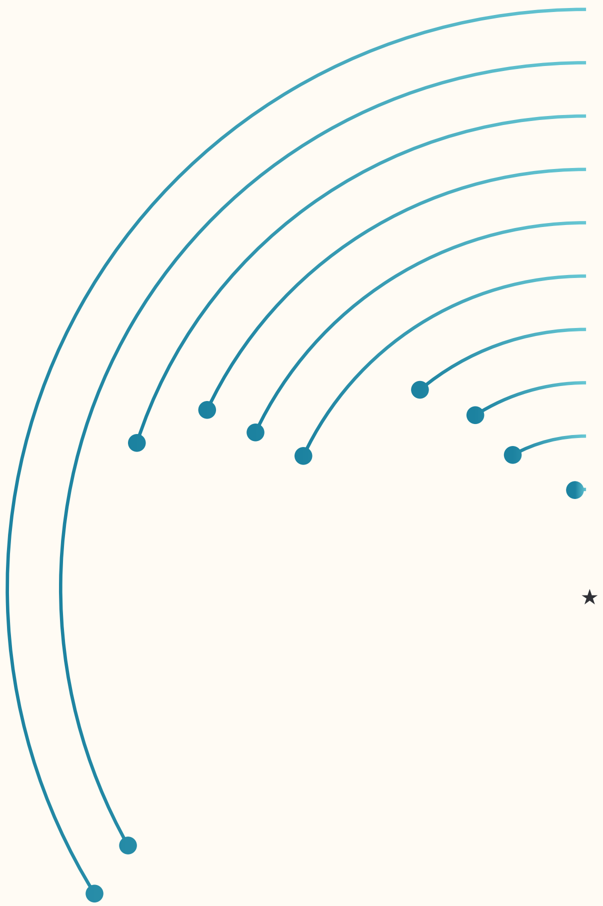
87% **of those already using biometrics** are open to using passkeys, compared to

57% **of those who don’t use biometrics.**

UNPACKING PASSWORDLESS

Consumers are confused about what “passwordless” actually means. That’s no surprise when we step back to consider the bevy of technologies offering new ways to access accounts – from magic links to facial recognition to physical security keys.

When consumers hear the word “passwordless,” here are the top terms that come to mind:



- **34%** Biometrics
- **33%** No login at all
- **20%** Passwords saved in a browser
- **18%** Password manager that stores passwords
- **18%** Passkeys that authenticate the user
- **18%** I don’t know
- **11%** Social sign-on (logging in with Facebook, Gmail, etc.)
- **9%** Magic links (signing in with a link sent by email or text)
- **8%** Physical security keys (such as YubiKey)
- **1%** Other

★ *Respondents were allowed to select multiple options.*

SIGNIFICANT SUBTLETIES

Many people associate biometrics with passwordless. The technologies are complementary, but they aren't the same thing.

Biometrics are the gatekeepers to information and credentials that are stored on your device. Today, that generally means unlocking access to stored passwords with a glance or a fingerprint, to save us the hassle of having to type them out each time.

Biometrics play the same gatekeeping role with passkeys, except there's no password behind the scenes. In short: passkeys protect your accounts, while biometrics protect access to your passkeys. Together, they represent a new approach to logging in that's easier, more secure, and nearly impossible for scammers to intercept. There's no password involved – period.

APPETITE FOR PASSWORDLESS

The general idea of passwordless logins is inherently appealing, as many people expressed interest in passwordless at the first mention – even without a widely accepted definition. Despite limited availability of the technology, some consumers are already experimenting with passwordless – and a solid majority are interested in trying more.

13%

say they already use passwordless technology.

58%

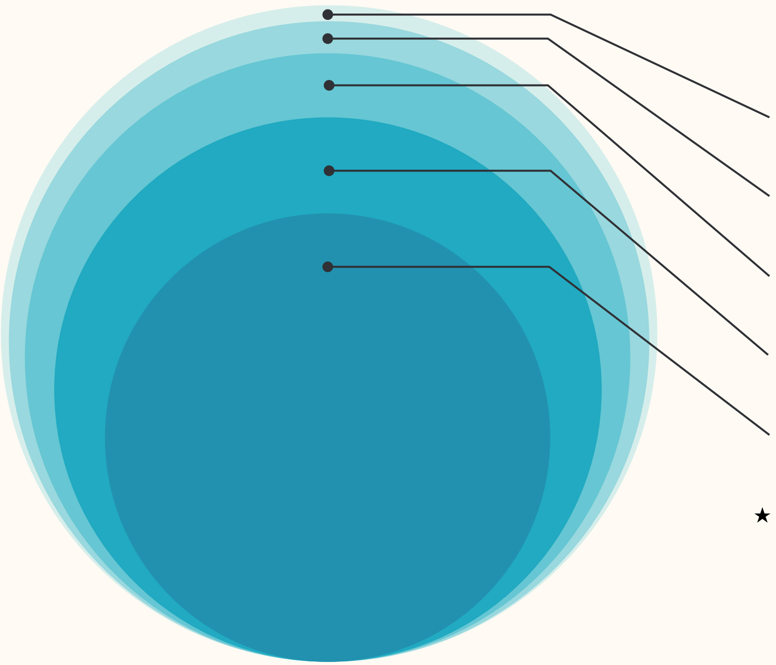
are open to using something other than a password to log in to their accounts.

CALIBRATING COMFORT

Consumers’ comfort with passwordless logins directly correlates with risk: People are more reluctant to use passwordless solutions for accounts that could expose them to greater personal harm. They’re more likely to experiment with using passwordless logins for throwaway and work-related accounts and least open to passwordless logins for sensitive financial accounts. **These sentiments point to the need for educating consumers on the security benefits of passwordless technology, as these benefits are even more important for sensitive accounts.**

We also found that the more consumers heard about passwordless, the more they warmed to the idea. Percentages below reflect perceptions of all respondents, after being asked about passwordless several times.

PASSWORDLESS READINESS



82% One-time “throwaway” accounts

81% Workplace

77% Retail

69% Healthcare/health insurance

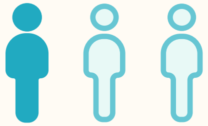
58% Financial services

★ *Percent of respondents at least somewhat open to using a method of logging in that doesn’t involve a password, for each type of account.*

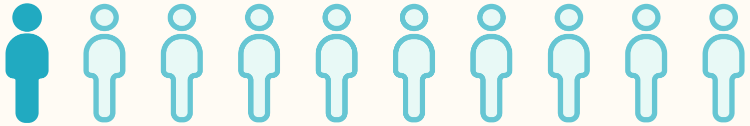
THE PASSKEY PROMISE

Within the passwordless realm, the idea of passkeys sparks a strong positive reaction from consumers – especially once they know what passkeys are and how they work. Despite most respondents’ lack of concrete experience with passkeys, they generally embraced the concept of logging in to any account simply using their device, with more powerful protections and far fewer headaches.

Three in four people (75%) indicate they’d be open to using passkeys, when shown a description and example.



One in three technology early adopters (35%) say they’d start using passkeys as soon as they come out.



One in 10 technology followers (11%) say they’d start using passkeys as soon as they come out.

03

Proof and consequences

Despite the great promise of passwordless technology, and strong interest in the potential of passkeys, consumers have understandable concerns about letting go of the familiarity of passwords. With their entire online lives at stake, and real-world consequences from breaches, consumers want assurances about security and backup options in case novel technologies don’t deliver.

Education can clearly help, but there’s nothing like a proven track record and strong word of mouth to spark greater adoption. Broader availability on popular websites, apps, and services will, of course, be essential.

SHOW ME THE SECURITY

Consumers' hesitancy about going passwordless ranges from questions about security, to concerns that they'll be locked out of critical accounts, to the simple fear of the unknown.

STRESSING SECURITY

34% don't think passwordless technology is secure.

46% would be motivated to adopt passkeys if they're proven to be more secure – pointing to the importance of educating consumers on passkeys' specific security benefits.

SEEKING BACKUPS

39% say they're worried that if passwordless technology doesn't work, they'll be locked out of accounts.

37% would be motivated to adopt passkeys if they had the option of using passwords as a backup.

UNCHARTED TERRITORY

28% say "fear of the unknown" is a hesitation they have about going passwordless.

55% say they'll always want to use passwords as a way to log in to select accounts.

GO PHISH

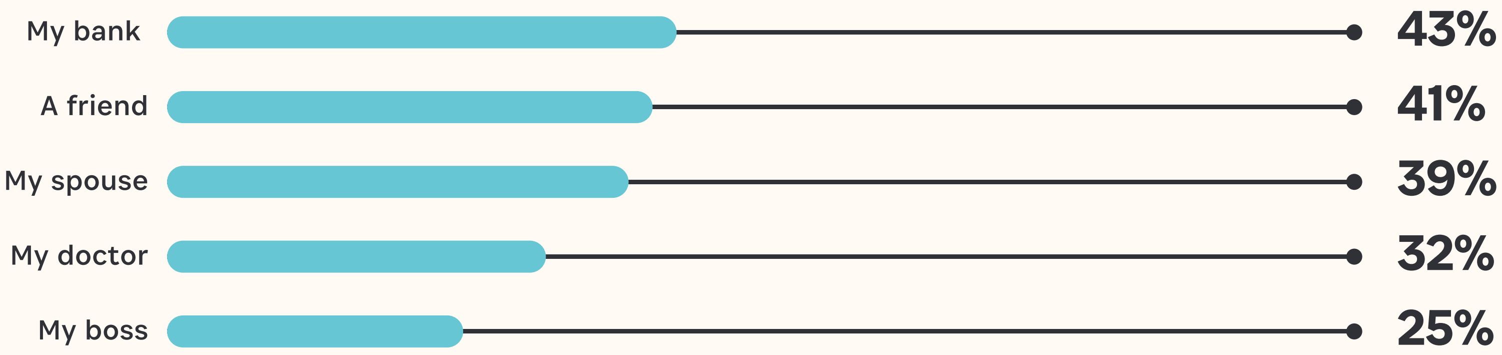
As attackers reduce the number of telltale typos and boost the production value of their fake missives, it's getting tougher to distinguish phishing attempts from legitimate messages.

In our survey, **a full 100% of respondents** said they either received a phishing message in the past year **(67%)** or know someone who did **(33%).**

One of the key benefits of passkeys is that they render phishing attacks obsolete. Without your physical device and a way to unlock it, scammers can't get the private key that's required to access your accounts – even if you're tricked into clicking on a scammer's link.

FAKE FRIENDS

Move over, boss. Finances and friends come first when it comes to separating us from our passwords. Consumers are most likely to fall for phishing that appears to come from their bank, a friend, or their spouse.



★ Percent of respondents who listed each source among the top three they'd be likely to fall for, in a phishing scam.

A PANOPLY OF PASSWORDLESS PERSPECTIVES

“My bank offers it, but I haven’t used it because I’m hesitant that something will go wrong.”

“I think it's fantastic and would eliminate the 35 passwords that I'm currently having to memorize.”

“I just hope it's secure, and that it doesn't make it easier for anyone to gain access to my accounts.”

“I generally like the idea of passwordless tech, but I am concerned about the security and potential privacy issues such as fingerprint scans and biometrics.”

Many survey respondents added thoughtful and wide-ranging comments detailing their questions, concerns, and perspectives on the promise of passwordless solutions.

“I really have no big concerns. I am all for things to help us make our lives easier.”

“I think in most cases it will be more secure than passwords I have trouble remembering, but there has to be some other way of logging in as a backup. For example, what happens when I die? Can my accounts be accessed by executors, etc.?”

“Change is always hard for some people, including me. I would hope that this has been thoroughly thought out and safety measures would be in place.”

CONCLUSION

Paving the way for a passwordless future

Most of us have become inured to the annoyances and risks of passwords, reluctantly accepting them as a frustrating and imperfect inevitability of modern life. But a better way to log in is beginning to take hold. Our research reveals a strong degree of openness to new technologies that relegate passwords to the past.

Consumers crave simplicity, but not at the expense of security. The beauty of passwordless solutions – and passkeys in particular – is their ability to deliver both security and simplicity at once, transforming our relationship with the online world.

A passwordless future is an alluring proposition, with the potential to make the process of logging in to apps, accounts, and online services far more seamless, user-friendly, and safe. If consumers' hopes about passwordless login solutions are backed up by knowledge, understanding, proof of security, and widespread availability, we'll see much more adoption of passwordless technology – and especially passkeys – in the months and years to come.

> "Passwordless technology brings great benefits for companies and their customers alike – making it easier to securely access online services while greatly reducing fraud and user frustration. This has been the mission of the FIDO Alliance since day one, with authentication experts from hundreds of companies, including 1Password, collaborating to make this vision a reality with passkey sign-ins."

—Andrew Shikiar, Executive Director and CMO, FIDO Alliance

METHODOLOGY

1Password conducted this research using an online survey prepared by Method Research and distributed by Dynata among 2,000 adults ages 18+ in North America (n=1,400 U.S. + n=600 Canada). The sample was equally split between gender groups with a balanced spread across age groups. A spread of geographies and race groups were included. Data was collected from January 25 to January 31, 2023.

ABOUT 1PASSWORD

1Password's human-centric security keeps people safe, at work and at home. Our solution is built from the ground up to enable anyone – no matter their level of technical proficiency – to navigate the digital world without fear or friction. The company's award-winning security platform is reshaping the future of authentication, including passwordless. 1Password is trusted by over 100,000 businesses such as IBM, Slack, Snowflake, Shopify, and Under Armour and protects the most sensitive information of millions of individuals and families across the globe. The company's ultimate goal is to help consumers and businesses get more done in less time – with security and privacy as a given. Learn more at 1Password.com.