

2022

Passwords & Authentication Consumer Trends Report



The following is an infographic summary of key findings from the 2022 Passwords & Authentication Consumer Trends Report based on data from a random double-opt-in survey of 2,000 general population Americans commissioned by Prove and conducted by market research company OnePoll in April 2022. For a deeper dive into the data, please skip to page 3 of the report.



2022

Passwords & Authentication Consumer Trends

Prove and OnePoll's 2022 Passwords & Authentication Consumer Trends Report reveals that the average American is tired of using multiple passwords to manage online accounts and is increasingly intolerant of slow identity verification processes.

Key Finding #1:

Customers Are Fed Up with Passwords

- 65% of Americans often or sometimes **felt frustrated while making an online account.**
- 34% of Americans said that they **would switch providers completely** if they were unable to log into their account easily.
- 62% of respondents said **they'd abandon trying to log into an account** after just 3 failed password attempts.



Key Finding #2:
Poor Password Hygiene is a Significant Security Risk

- 79% of respondents have **six or fewer go-to passwords** across all of their online accounts.
- 60% of Americans believe **they could guess their significant other's password in 6 attempts or less!**
- 22% More than one in five (22%) **have been a victim of identity fraud.**

Key Finding #3:

Accelerate Your Onboarding... Or Else



- 69% of Americans feel that the **speed and ease of the customer experience is important.**
- 51% of respondents said they **would switch brands as a result of slow identity verification.**
- 33 seconds, was the **average time respondents believe it should take to create an account online.**

Key Finding #4:
Customers Prefer Phone (Mobile)-Based Authentication to Passwords

- 64% of respondents said that **authentication through their phone is a more convenient option than passwords.**
- 44% said the **ability to open or use an account from their mobile phone or device** was an important factor when completing a new online account application.
- 38% The **most preferred way of authenticating identity in the Metaverse was through phone signals (38%)** vs. passwords (30%), SMS text codes (13%), and biometric authentication (9%).

The Bottom Line

Consumers are fed up with passwords and slow identity verification and are looking for solutions that will provide a superior user experience. For more information about [advanced identity authentication methods that enable companies to go beyond the password](#), visit [prove.com](#)



The 2022 Passwords & Authentication Consumer Trends Report highlights data from a random double-opt-in survey of 2,000 general population Americans commissioned by Prove and conducted by market research company OnePoll in April 2022. The survey reveals that **the average American is tired of using multiple passwords to manage online accounts and is increasingly intolerant of slow identity verification processes.** Other key statistics about respondents' attitudes towards passwords and identity verification and authentication include:

- Respondents had an average of **four “go-to” passwords** -- with 31% saying these are just different variations of the same password.
- **62% of U.S. consumers said they'd abandon trying to log into an account** after just three failed password attempts, **51% would switch brands as a result of slow identity verification**, and **34% would switch providers completely** if they're unable to log into their account easily.
- In terms of password security, respondents said they felt they **could hack their significant other's devices in just five attempts.**
- From a customer experience perspective, **64% of those polled said that authenticating their identity through their phone is more convenient than using a password.**
- More than **one in five (22%) have been the victim of identity fraud** and another 36% know someone who has.

Additional survey findings related to the **importance of the digital customer experience** include:

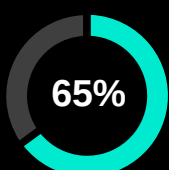


- **45% believe it should take less than 30 seconds** to create a new online account.
- **69% of Americans feel that the speed and ease of the customer experience** when signing up for new financial products such as a credit card, bank account, or cryptocurrency account **is somewhat or very important.**
- **44% said the ability to open or use an account from their mobile phone or device** was an important factor when completing a new online account application.
- **The most preferred way of authenticating identity in the Metaverse was through phone signals (38%)** vs. passwords (30%), SMS text codes (13%), and biometric authentication (9%).

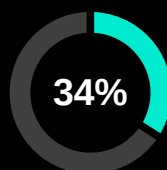
Key Finding #1:

Customers Are Fed Up with Passwords

- **65% of respondents** either “often” or “sometimes” **feel frustrated as a result of passwords.**
- **34% of respondents** report that they **would switch providers completely** if they were unable to log into their account easily and **51% would switch brands as a result of slow identity verification.**
- **62% of U.S. consumers said they'd abandon trying to log into an account** after just 3 failed password attempts.



of Americans often or sometimes felt frustrated by passwords



of Americans said that they would switch providers completely if they were unable to log into their account easily.

Source: 2022 Passwords & Authentication Consumer Trends Report, Prove & OnePoll

Key Finding #2:

Poor Password Hygiene is a Significant Security Risk

79% of respondents have six or fewer go-to passwords across all of their online accounts. This leads to what cybersecurity professionals call the [domino effect](#).

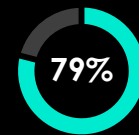
What's the domino effect?

"A domino effect can result as one site's password file falls prey to a hacker who then uses it to infiltrate other systems, potentially revealing additional password files that could lead to the failure of other systems."

Source: The Domino Effect of Password Reuse, Communications of the ACM

Poor password hygiene is so common that over **60%** of Americans believe they could **guess their significant other's password in 6 attempts or less!**

Source: 2022 Passwords & Authentication Consumer Trends Report, Prove & OnePoll



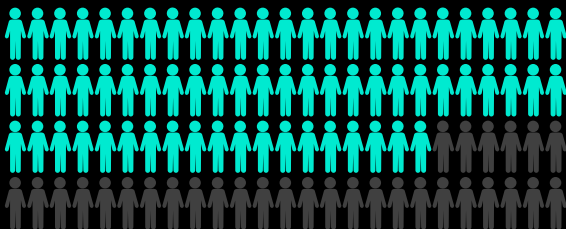
79% of Americans had six or fewer go-to passwords

Key Finding #3:

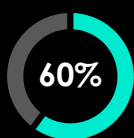
Accelerate Your Onboarding... Or Else

When it comes to onboarding new customers, companies are in a race against the clock.

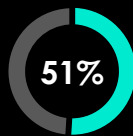
- **51% of respondents said they would switch brands** as a result of slow identity verification.
- **69% of Americans feel that the speed and ease of the customer experience** when signing up for new financial products such as a credit card, bank account, or cryptocurrency account **is important**.
- Respondents believe it should take about **33 seconds to create a new account online**, but almost half (45%) will cap it at 30 seconds or less.



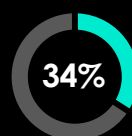
69% of Americans feel that the speed and ease of the customer experience is important



60% Would abandon trying to log into an account after 3+ tries



51% Would switch brands as a result of slow verification



34% Would switch providers completely if they're unable to log into their account easily

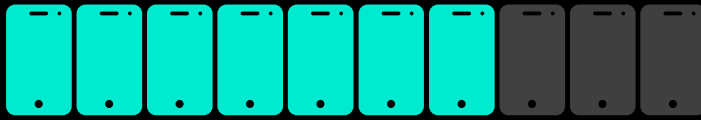
Source: 2022 Passwords & Authentication Consumer Trends Report, Prove & OnePoll

Key Finding #4:

Customers Prefer Phone (Mobile)-Based Authentication to Passwords

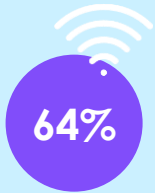
The results are clear: mobile-based authentication methods are the future.

- **64% of respondents said that authentication through their phone is a more convenient option than passwords.**
- **71% said that having a more straightforward sign-in process with facial recognition is more convenient and user-friendly** than creating new profiles and passwords.



Source: 2022 Passwords & Authentication Consumer Trends Report, Prove & OnePoll

7 in 10 respondents agreed that having a simpler sign in with facial recognition is more convenient and user friendly than creating new profiles and passwords



64% of Americans say authenticating through their phone is more convenient than passwords

Source: 2022 Passwords & Authentication Consumer Trends Report, Prove & OnePoll

- **Three-quarters of respondents said that biometric authentication is more secure overall than a traditional password.**
- **44% said the ability to open or use an account from their mobile phone or device** was an important factor when completing a new online account application.
- The **most preferred way of authenticating identity in the Metaverse was through phone signals (38%)** vs. passwords (30%), SMS text codes (13%), and biometric authentication (9%).

"As we have all seen, the security that online businesses use is overly tedious, and yet not very secure," said Prove Chief Executive Officer, Rodger Desai. "The bottom line for consumers? Complicated doesn't mean secure. The solution is actually sitting in the pocket of most adults – their cell phones. With Prove, your phone becomes by far the most secure, accurate, and frictionless way to prove identity – and our survey demonstrates that consumers would prefer the convenience of the phone in their pocket."



Rodger Desai, Chief Executive Officer
and Co-Founder of Prove

The Bottom Line

Consumers are fed up with passwords and slow identity verification and are looking for solutions that will provide a superior user experience. For more information about [advanced identity authentication methods that enable companies to go beyond the password](#), visit prove.com

