

What are passkeys? Experience the life-changing magic of going password-less

Here's how to take the first steps toward ditching passwords for good





Next-generation account security

Based on FIDO Alliance and W3C standards, passkeys replace passwords with cryptographic key pairs. These key pairs profoundly improve security.

Strong credentials. Every passkey is strong. They're never guessable, reused, or weak.

Safe from server leaks. Because servers only keep public keys, servers are less valuable targets for hackers.

Safe from phishing. Passkeys are intrinsically linked with the app or website they were created for, so people can never be tricked into using their passkey to sign in to a fraudulent app or website.

In iCloud Keychain, passkeys are end-to-end encrypted, so even Apple can't read them. A passkey ensures a strong, private relationship between a person and your app or website.



Works alongside passwords

Since signing in with passkeys uses AutoFill and Face ID or Touch ID for biometric verification, the transition to passkeys is seamless. This lets people use passkeys alongside passwords, so you don't need to adjust your sign-in page based on credential type. You'll use the new Authentication Services API to add passkeys, creating sign-in flows that are familiar to users.

TECH Updated Mar 5, 2024 at 9:28 AM PST

Passkeys: all the news and updates around passwordless sign-on

By [Jess Weatherbed](#), a news writer focused on creative industries, computing, and internet culture. Jess started her career at TechRadar, covering news and hardware reviews.

[Link](#) [Facebook](#) [Twitter](#) [RSS](#) [2 Comments \(2 New\)](#)

The need to remember lengthy, complicated passwords to sign into your accounts could soon be a thing of the past thanks to passkeys: a new login technology that replaces passwords with authentication mechanisms built into your own devices. That means you can use Face ID on your iPhone, Windows Hello on your PC, or the fingerprint sensor on your Android phone to authorize access to your websites, apps, and services — providing they support passkey sign-on.

Passkeys are built on WebAuthn (or Web Authentication) tech and stored directly on your device. They are supported by companies like Apple, Google, and Microsoft because they're more secure than passwords or PINs which can be stolen. Password managers can help backup and sync passkeys across all your devices.

...that passkeys will eventually replace passwords entirely. ...some time. Here you can follow all the updates ...ies have rolled out

Passkeys – The Future of Online Security



Changing the Nature of Authentication

The FIDO ("Fast IDentity Online") Alliance launched in February 2013



The FIDO Alliance is a non-profit open industry association with a focused mission: **REDUCE THE WORLD'S RELIANCE ON PASSWORDS**

The FIDO Alliance is changing the nature of authentication with open standards (WebAuthn) for phishing-resistant sign-ins with passkeys

FIDO runs certification programs that maintain quality and oversight of password less adoption



FORGOT YOUR
PASSWORD?

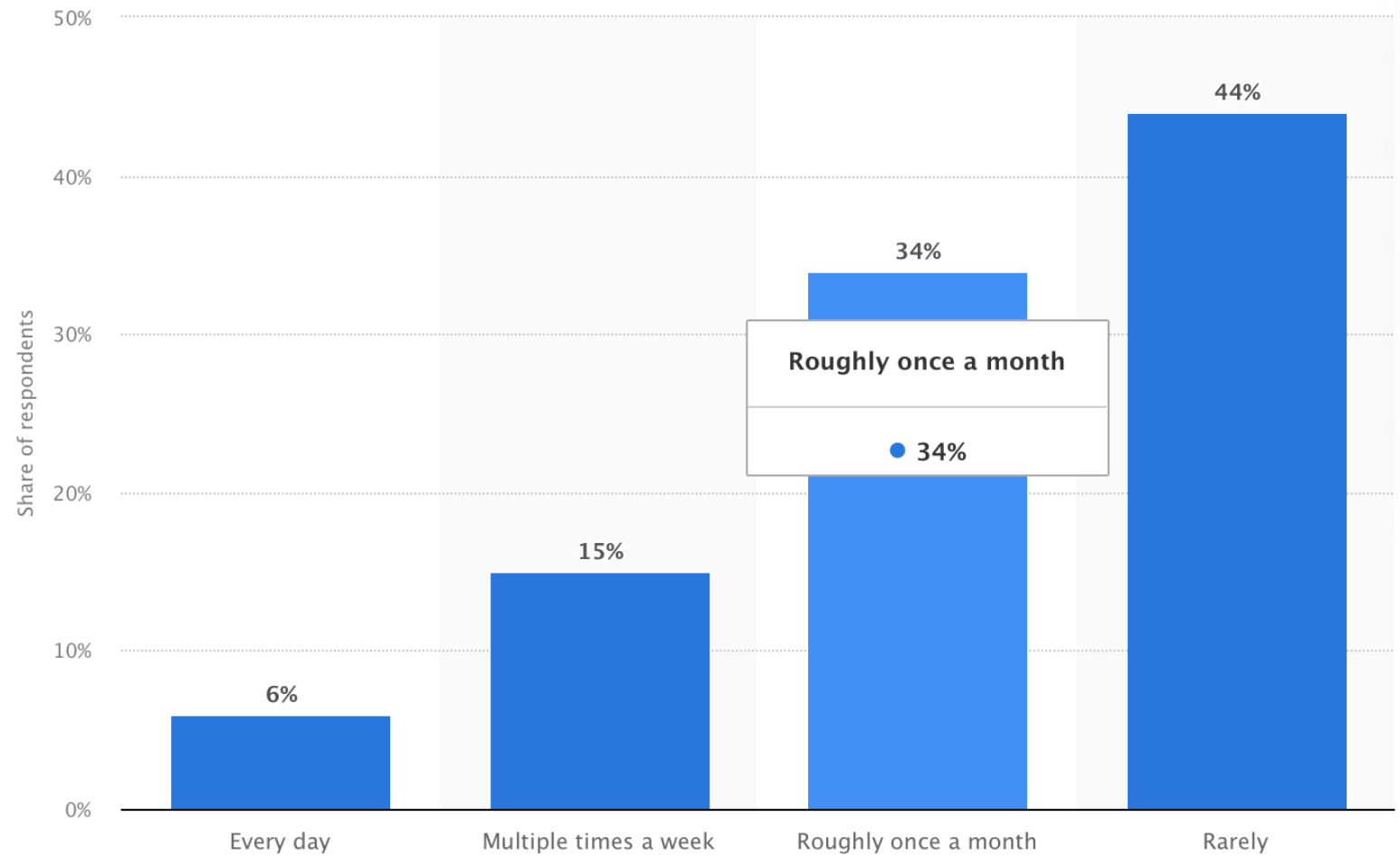


Forgot your password

- Passwords are the most common authentication mechanism in use today
- Almost every online site and application requires users to enter a password to gain access to their account
- The average person is locked out of ten online accounts per month due to a forgotten password
- Password resets provide a solution; however, 57% of people claim that they will forget the new password immediately after the reset

If you create a complicated new password, you're likely to forget it again. If you reuse an existing one, you're putting your security at risk

Frequency of resetting passwords worldwide in 2022



Sobering Statistics on Password Usage

When our primary factor is passwords...

81%

of hacking-related breaches
are caused by weak or stolen
passwords
(Ping Identity)

43%

Gave up on a purchase because
they forgot their password (FIDO
Alliance)

76%

Rise in direct financial loss from
successful phishing attacks
from 2022-2023 (Proofpoint)

64%

either using weak passwords or repeat
variations of passwords (Keeper)

Easily phished or socially engineered, difficult to use and maintain

52%

of consumers are
aware of passkeys

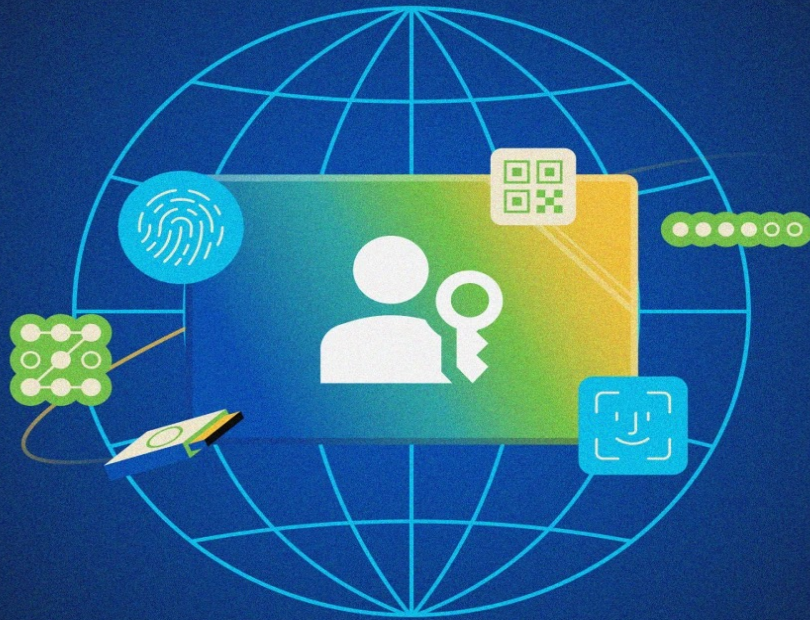
84%

of IT leaders said they
are familiar with
passkeys

92%

of IT leaders said
passkeys would benefit
their overall security
posture

Passkey Awareness



LEVELS OF ACCOUNT SECURITY

(worst to best)

Memorized Passwords	Susceptible to phishing, brute force hacking, password reuse, server hacks - DON'T DO THIS!
Password Manager	Better, but still susceptible to phishing and server hacks (think LastPass)
Password Manager with 2FA Enabled (e.g., Duo)	Getting better, but NOT perfect; can still be phished or server hacked
Synced Passkeys (multi-device credentials)	Getting warmer; shareable; can't be phished, server leaks don't matter (website has only the Public Key)
Hardware Bound Passkeys (single-device credentials)	Most secure option; not shareable or able to copy; requires presence of a physical device (e.g. YubiKey); DO NOT lose your key as it's difficult to regain access; best to have 2 (a backup key)



What are Passkeys?

- **Passkeys are a new type of login credential that allow you to log in to websites and apps without having to enter a password**
- **With passkeys, you sign in to applications and websites with a biometric sensor (such as a fingerprint or facial recognition), or PIN, freeing you from having to remember and create and manage passwords**
- **When passkeys are correctly fully implemented, you don't have to type anything out...not even a username**
 - **You don't have to enter a two-factor authentication code**
 - **And you don't have to worry about whether someone is trying to trick you with a scam website**

How Passkeys Work



- They use public key cryptography to create a key pair, matching a private key on the user's device with a public key stored on the website or application servers
- To use passkeys, you need a device that can generate and store them, e.g. a smartphone, a laptop, or a tablet
- Passkeys are one of the most secure authentication methods available
 - Passkeys are unique to each website or application (service)
 - Private key is stored on your device instead of on a server
 - They cannot be guessed, phished, or stolen by hackers; can be shared
- Devices with Touch or Face ID, allow biometrics to authorize use of the passkey, which authenticates the user to the application (service) or website



How Do I Setup a Passkey?

- **Setting up a passkey is simple and secure**
- **Steps will vary depending on the website or app as well as your device and Operating System – **Note****
- **General guidelines:**
 - ✓ **First, find a website or app that supports passkeys**
 - ✓ **If a new account, enter your email, select Create Account, choose "Create a Passkey"**
 - ✓ **If an existing account:**
 - ✓ **Sign-in with your existing credentials**
 - ✓ **Navigate to Security Settings (e.g., Profile)**
 - ✓ **Select "Create a Passkey"**

Note:

<https://www.passkeys.io/compatible-devices>

What software on my device creates the passkey?

- Depends on the type of device and the operating system you have
- For example...
 - For a Windows device, the passkey is created by the Windows Hello feature, which uses biometric or PIN authentication to unlock your passkey
 - For an Android device, the passkey is created by the Google Smart Lock feature, which uses your device's biometrics, such as fingerprint or face recognition, to unlock your passkey
 - For an iOS device, the passkey is created by the iCloud Keychain feature, which uses Face ID or Touch ID to unlock your passkey
- Alternatively, you can use a password manager, such as 1Password or Bit Warden, to create and store your passkeys
 - These apps use a master password or biometric authentication to access your passkeys
 - Password Managers can sync passkeys across your different devices

Examples of Passkey Login

- **Ways you can use passkeys to login to apps and websites w/o using a username and password combination**

- ❖ **Fingerprint recognition (Touch ID)**
- ❖ **Face recognition**
- ❖ **Iris recognition**
- ❖ **Speech recognition**
- ❖ **Screen lock pins**



NO: ONE PERSON
GENDER: FEMALE
AGE GROUP: YOUNG WOMEN
ETHNICITY: CAUCASIAN
HUMAN BODY PART: HUMAN FACE
TIME: 331 S
DETECTION: 25621 POINTS

Passkeys vs Security Keys – Different or Same?

- Security keys are physical tokens that utilize strong public key cryptography and provide robust defense against phishing and credential theft
- Software based passkeys aim to enhance security and user experience by leveraging familiar device unlock methods such as biometrics (e.g., fingerprint or facial recognition) or PINs
- Both passkeys and security keys offer significant improvements over traditional password-based authentication; both are FIDO2 certified
- Choosing between passkeys and security keys requires user consideration of various aspects, including security, usability, convenience



Single-Device Credential)

Passkey Log-in Sequence

Private key



Public key



May or may not require Username

1 Login request

2 Challenge

4 Response (signed with private key)

5 Login complete

3 Login request approved by FaceID or TouchID (depending on model)



www.mysite.com

Why Passkeys Are Better Than Passwords

PASSWORDS

VS

PASSKEYS

- **Security** - Passkeys are more secure than passwords because they use advanced cryptography and biometric authentication
 - They cannot be guessed, phished, or stolen by hackers
 - They also protect you from malicious websites that try to trick you into entering your passwords
- **Convenience** - Passkeys are more convenient than passwords because they let you sign in with just your fingerprint, face, or screen lock(PIN)
 - You don't have to remember or type complex passwords for each of your accounts
 - You can also sync your passkeys across your devices, so you can log in from anywhere
- **Privacy** - Passkeys are more private than passwords because they do not rely on human-readable shared secrets that are transmitted over the internet
 - Your biometric data stays on your own device and is not shared with the services you use
 - You also have more control over your personal information and online identity

How passkeys are shared

- **With a dedicated password manager, users can share their passkeys with anyone, no matter what devices they use**
- **Create a Password Manager shared vault and everyone with access to that vault will be able to access the passkeys stored there**
- **Unlike single-device credentials which are passkeys that are bound to a single device (think YubiKey)**
- **Multi-device credentials are passkeys that can be moved and synced between devices (think Apple Keychain or Google Password Manager)**



Disadvantages of Using Passkeys

- **Risk of device loss or theft – May lose access to your accounts**
- **Limited application - Passkeys are not currently supported by all websites and services**
- **Biometrics issue - Passkeys rely on biometric authentication... fingerprint or face may change over time (unable to scan)**
- **User adoption - Passkeys are a new and unfamiliar technology for many users...may be time-consuming and frustrating**



Biometrics are flawed

- Irreplaceable
- Irrevocable
- Can change
- Cannot be transferred
- Are breakable

Malaysia car thieves steal finger

By Jonathan Kent
BBC News, Kuala Lumpur

Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.








Upgrading to a new smartphone?

- **Passkeys are easily transferred over to a new device**
- **Passkeys are stored in your iCloud Keychain, if upgrading to a new iPhone, just log in using your Apple Id on the new device**
- **On Android, when you set up a new smartphone, your passkeys are securely transferred when you move the rest of your apps and data to the new device**
- **Password Managers store their data in the cloud**

What Sites Currently Allow Use of Passkeys

- **Setting up passkeys on your smartphone or computer requires finding sites and services that support their use**
- **A “passkey directory” exists that users can contribute to; it is searchable, making it easy to find out whether a company (web site) offers passkey support**
- **Can expect additional sites/apps to announce support of passkeys**

The screenshot shows the homepage of Passkeys.directory. At the top, the title 'Passkeys.directory' is displayed in a large, white font against a gradient background. Below the title, a subtitle states: 'Passkeys.directory is a community-driven index of websites, apps, and services that offer signing in with passkeys.' A button labeled 'Provided by 1Password' is visible. The main content area features a search bar with the placeholder text 'Search passkeys.directory', which is highlighted with a green border. To the right of the search bar are filters for 'Viewing' (set to 'All listings') and 'Sort by' (set to 'Name'). Below the search bar, there is a section titled 'Suggest a missing app or service' with a description and a '+ Suggest new listing' button. The bottom section is a table listing supported services.

NAME	SUPPORTED	CATEGORY	
 Adobe adobe.com	Sign In	Information Technology	Details
 Air New Zealand airnewzealand.co.nz	Sign In	Travel & Tourism	Details
 Amazon amazon.com	Sign In	eCommerce	Details



Will Passkeys Replace Passwords?

- **Weak or reused passwords can put both people and the companies they work for at risk**
- **Transition from passwords to passkeys will likely take time**
- **Passkey support is built into modern computing devices today and is being endorsed industry wide by major players**
- **You can start using passkeys for your online accounts today to make them more secure to stay one step ahead of hackers**

Life Without Passwords

<https://youtu.be/IRFeuSH9t44>

The logo for Passkeys, featuring a white silhouette of a person's head and shoulders next to a white key icon.

Passkeys

Passkeys – Here to Stay

- Increasingly digitized world will necessitate the need for secure and reliable authentication
- Passkeys offer convenience and simplicity for users as well improved security
- If security isn't convenient, users will find ways around it, thus increasing security risks
- Authentication using unique biometric data or codes enable passkeys to become more prevalent in our daily lives
- The adoption of passkeys by major tech companies such as Apple, Microsoft, and Google validate their importance and potential as an authentication method
- Passkeys are here to stay and have the potential to change the future of authentication





Extra Credit – Self-Study

- **FIDO Multi-Device credentials in Action**

<https://youtu.be/SWocv4BhCNg?si=ow2cSun6jj0Oq31c>

- **How to Use Passkeys on iPhone, iPad, and Mac**

<https://youtu.be/HVYESg1Qrr0?si=1y3wew6Lzv1IjzYD>

- **How do passkeys work? (includes a neat demo video)**

<https://www.passkeys.io/technical-details>



Extra Credit – Self-Study

- **Accelerating the Availability of Simpler, Stronger Passwordless Sign-Ins (great list of FAQs)**
<https://fidoalliance.org/paskeys/>
- **Passwords vs. Passkeys - FIDO Bites Back!**
<https://youtu.be/9nrE4t4-IXA>
- **Everything you need to know about the death of passwords**
<https://www.tomsguide.com/news/what-are-passkeys>
- **The Future of Passwordless Authentication**
<https://www.esecurityplanet.com/applications/what-is-a-passkey/>



Extra Credit – Self-Study

- **What the !#@% is a Passkey?**
<https://www.eff.org/deeplinks/2023/10/what-passkey>
- **Everything You Need To Know About Passkeys from Yubico (Yubikey)**
https://resources.yubico.com/53ZDUYE6/at/prhsnwrpw2j8s9gjnxvrcmv/Yubico_Passkey_Infographic.pdf?format=pdf

QUESTIONS

fidoTM
ALLIANCE