Created by Claude 2026-03-05

Understanding Passkeys

A Plain-English Guide to a Simpler, Safer Way to Log In

What Is a Passkey?

A passkey is a modern replacement for the traditional password. Instead of creating and memorizing a string of letters, numbers, and symbols, a passkey lets you log in to websites and apps the same way you unlock your phone or computer — with your fingerprint, your face, or a simple PIN.

That's really all there is to it. When a website asks you to log in, you simply look at your phone or touch the fingerprint sensor, and you're in. No typing required.

> **The simple version:**
> A passkey is like a digital key that lives in your phone or computer. It's created automatically, it's unique to each website, and only YOU can use it — because it requires your fingerprint, face, or device PIN to work.

Why Are Passkeys Better Than Passwords?

Passwords have a fundamental problem: they can be stolen, guessed, or leaked. Passkeys eliminate these risks entirely.

Traditional Password	Passkey
You create and remember it	Your device creates it automatically
Can be stolen by fake websites	Cannot be tricked by fake websites
Can be guessed or cracked	Mathematically impossible to guess
Same password used on multiple sites (risky)	Each site gets a unique passkey
Requires you to type something	Just use your fingerprint or face

One of the biggest advantages: passkeys cannot be phished. "Phishing" is when a criminal sends you to a fake website that looks like your bank or email, hoping you'll

type in your password. With passkeys, your device automatically knows if a website is legitimate — and will simply refuse to log you in to a fake site.

How Do They Actually Work? (No Tech Jargon)

You don't need to understand the technical details, but here's a simple analogy that captures the idea:

> **Think of it like a lock and key:**
> When you set up a passkey, your device creates two things simultaneously: a "lock" that gets sent to the website, and a "key" that stays only on your device. When you log in, the website shows your device the lock. Your device uses the key to open it — proving it's really you. The key never leaves your device, so no one can steal it over the internet.

Because the key never travels across the internet, there's nothing for hackers to intercept. And because each website gets a different lock-and-key pair, a security breach at one website doesn't affect your other accounts.

Where Can You Use Passkeys?

Passkeys are already supported by many major services, and more are adding them every day. As of 2025, you can use passkeys with:

- Google (Gmail, Google Drive, YouTube, etc.)
- Apple (Apple ID and iCloud)
- Microsoft (Windows, Outlook, Microsoft 365)
- Amazon
- PayPal
- GitHub
- Many banks and financial institutions
- Numerous other popular websites and apps

You don't have to switch all at once. You can set up a passkey for just one account to try it, and keep using passwords elsewhere in the meantime.

How to Set Up a Passkey

The exact steps vary slightly by website, but the general process is simple and takes about one minute:

1. **Log in to the website** using your existing username and password as you normally would.
2. **Go to your account settings** — usually found under "Security," "Sign-in options," or "Privacy."
3. **Look for a "Passkey" option** and click "Add a passkey" or "Create a passkey."
4. **Confirm with your fingerprint, face, or device PIN** when your device prompts you.
5. **Done.** From now on, you can log in to that website with just your fingerprint or face.

Common Questions

What if I lose my phone?

Your passkeys are automatically backed up to the cloud — Apple iCloud if you use an iPhone, Google if you use an Android phone. When you get a new phone and sign in to your account, your passkeys will be there waiting for you. You won't lose access to anything.

What if a website doesn't have passkeys yet?

No problem — just keep using your regular password for that site. Passkeys and passwords can coexist. You only use passkeys where they're available, and passwords everywhere else.

Do I need to remember anything new?

No. That's the whole point. You don't need to create, remember, or store anything. Your device handles everything automatically. The only thing you need to do is be you — use your fingerprint, face, or the PIN you already use to unlock your device.

Are passkeys really more secure than a strong password?

Yes — significantly so. Even a strong, complicated password can be stolen from a website's database or captured on a fake website. A passkey cannot be stolen

remotely, cannot be guessed, and cannot be used on a fake site. Security experts widely consider passkeys to be the biggest improvement in account security in decades.

A Good Way to Get Started

If you'd like to try passkeys, Google is an easy place to start, since many people use Gmail. Here's how:

- Go to myaccount.google.com on your computer or phone
- Click "Security" in the left menu
- Scroll down and look for "Passkeys"
- Click "Create a passkey" and follow the prompts
- The next time you sign in to Google, you'll be asked to use your fingerprint or face instead of your password

Bottom line:

Passkeys are simpler than passwords (no typing, no memorizing) and far more secure. They're already here, they work well, and setting one up takes about a minute. The future of logging in is your face or your fingerprint — and that future has already arrived.