How passkeys actually work

No jargon. No magic.
Just a clever lock-and-key trick.

Step 1 You create a passkey

Your device → creates → **Private key** — Stays on your device. Never leaves. Ever.

Public key — Gets sent to the website. Useless on its own.

Step 2 You log in

Website → sends a challenge → Your device checks it's really you (or) → sends back signed proof → Website checks with public key → You're in!

No password was typed. No password was sent. Nothing to steal.

Why this stops hackers

Fake website sends you a link

Your device says: "Wrong site."

OR

A website you use gets hacked

Hackers only get the public key

Your passkey is tied to the real website. Fakes don't match.
A stolen public key is like a stolen padlock — useless without the key.

But what about Google / Apple / Microsoft?

Your device — Private key lives here → syncs → iCloud / Google cloud — Encrypted blob → Apple / Google can see the blob but can't read it

When your passkey syncs between your devices, it's encrypted end-to-end.

The cloud stores a locked box. Only your devices have the key to open it.

Apple, Google, and Microsoft literally cannot see your private key.
That's the difference between "stored in the cloud" and "readable in the cloud."

riskready