

Here's how to secure your Twitter account without paying for Blue

If you've been on Twitter lately, you might've seen a message prompting you to switch away from text message two-factor authentication (2FA). That's because Twitter's putting the feature behind a paywall, which means you either have to pay \$8 per month for Blue or switch to another authentication method – and I think most of us would choose the latter.

Fortunately, SMS 2FA isn't the only way to secure your Twitter account, with other methods still available for free. The platform's shutdown of the feature – at least for non-Blue subscribers – is actually a good reminder that we shouldn't be using it in the first place.

SMS 2FA leaves you vulnerable to SIM-swapping attacks, which usually happen when a bad actor uses social engineering or other access to get your mobile carrier to reassign your phone number to them. Once they've gained access to your number, the hacker can intercept the verification codes you receive over text messages or through phone calls when you try signing into your accounts, potentially allowing them to log in instead.

a:hover]:shadow-highlight-franklin dark:[&a:hover]:shadow-highlight-franklin [&a]:shadow-underline-black dark:[&a]:shadow-underline-white">What are Twitter's other 2FA options?

Aside from SMS 2FA, you can either use an authenticator app or a security key as an extra layer of protection when logging into your Twitter account.

Authenticator apps, like Authy, Google Authenticator, and Microsoft Authenticator, typically generate one-time passwords (OTP) that change after a short period of time. Just like SMS 2FA, you can use these codes to access your accounts on the web, but you'll find them in the app – not in your text messages. They also change quite frequently, so you'll have a much more limited amount of time to enter them.

While this solution still isn't immune to attacks, it's safer than SMS 2FA, as it's more difficult for a hacker to get access to the physical device where the authenticator app's installed.

Security keys, on the other hand, are one of the safest forms of 2FA because the key itself verifies the service as valid to help prevent phishing, and it can be more convenient than copying over a constantly rotating code. However, this method requires you to purchase a physical piece of hardware that you insert or connect wirelessly to your phone or computer. This key verifies your identity when logging into your account.

How you use the key largely depends on the one you purchase, as some come with support for USB-C, USB-A, and Lightning, while others support NFC. Many security key brands, , are compatible with Twitter, but it's worth checking whether the key you're eyeing supports the sites you need it for.

You can read about security keys in more detail, including how to enable them for Twitter, in this post [here](#).

a:hover]:text-black [>a:hover]:shadow-underline-black dark:[>a:hover]:text-gray-e9 dark:[>a:hover]:shadow-underline-gray-63 [>a]:shadow-underline-

**gray-13 dark:[&>a]:shadow-underline-
gray-63">Choose *"Authentication app"* to
get started.**