How to Protect Yourself from a SIM Swap Attack

Last Modified on 05/10/2025 3:11 am EDT

Multi-factor Authentication (MFA) is a critically important security feature that all cryptocurrency users should be employing, at the very least on all semi-important financial accounts and email accounts. SMS 2FA is but one type of MFA that is commonly available. Unfortunately, it is not a particularly good form of MFA as it prone to being defeated by a SIM Swap attack. So how can one protect themselves from a SIM Swap Attack?

Answer: There's no widely available way that users can take to avoid becoming a victim of a SIM Swap. However, there are steps users can take to drastically reduce the damage a SIM Swap can do -- in many cases it can render a SIM Swap harmless and nothing more than a minor inconvenience.

To avoid a SIM Swap attack, avoid using SMS 2FA, especially on financial accounts, crypto exchange accounts and all email addresses. Opt for a more secure form of MFA instead. Options include app-based authenticators like Google Authenticator, Authy, and Duo Mobile. Prompt-based authenticators are also good options that are commonly available. Hardware-based authenticators like Yubikeys are also a good option, but Yubikeys aren't free, unlike the other aforementioned forms of MFA.

In some jurisdictions, there are cell phone providers that are less prone to SIM Swap attacks. In the U.S. Efani is an example of this, although it does come at a premium price. Google Fi is also known to be less prone SIM Swap attacks, but isn't widely available throughout the US.