Multi-factor Authentication (MFA) Recommendations and Advice

10/25/2024 12:29 am EDT

Utilizing adequate Multi-factor Authentication (MFA), particularly for any accounts with any links to cryptocurrency accounts or financial accounts is critically important for users to implement in order to ensure accounts are relatively secure and much less prone to being hacked or compromised.

Some types of MFA are inherently better or more secure than others.

Hardware-based MFA such as Yubikey are generally considered to be the most secure type of MFA, but also one of the least frequently used since they do cost money, and additionally can be slightly less convenient since if you are trying to access an account and don't have the hardware device with you at the time, then you won't be able to pass MFA.

Time-based-one-password (TOTP) **App-based MFA** such as Google Authenticator, Authy, Duo Mobile, and Microsoft authenticator are generally strong and secure forms of MFA, as long as they are set up correctly. It's a good idea to set up and utilize app-based authenticators on accounts if not already doing so, however it should be kept in mind that depending on the settings a user chooses in these apps, there are are rare instances where MFA can be compromised. For Authy, that vulnerability is the multi-device feature. For Google Authenticator, the issue is that depending on your settings, your Google Auth 2FA codes may be backed up to the cloud. Ergo, it's critically important to pay attention to the settings of your authenticator app, and to set it up in a way such that the 2FA codes it stores won't be at risk of compromise.

Prompt-based MFA is also a strong and secure form of MFA. Google Prompt and the Coinbase app itself both offer prompt or push notifications to a users' device to authenticate logins. The issue is that generally each account you have will require it's own app for push notifications, and many accounts users have will not have an associated applications that offers prompt-based MFA at all. Since it is common for users to have dozens, or even hundreds of accounts, and users don't want an app for each account (if there is an app available at all), prompt-based MFA simply can't be a MFA solution for all accounts, but can be a good solution for some.

SMS-based MFA is arguably the least secure form of MFA, and is best to avoid using this type of MFA if possible. It is prone to being compromised due to fraudulent SIM Swaps, which would result in the attacker received 2FA codes to their phone, which they can then use to log into your accounts and to perform fraudulent password resets.

Utilizing **Email MFA** is potentially problematic because during the course of a hack or account takeover, it's common for the hacker to obtain control of email addresses of a victim, which would in turn give the hacker access to authentication codes or links sent to the email address. If using email MFA, it's critically important to also use an additional more secure form of authentication in conjunction with it.

Ensure you are using strong forms of MFA on all cryptocurrency accounts, financial accounts, and also email accounts. A breach of an email account often occurs prior to cryptocurrency accounts to be compromised -- if your email account remains secure, protected by MFA, and isn't prone to a fraudulent recovery attempt, there's a good chance that this may prevent an attacker from getting access to your cryptocurrency exchange accounts.