# Sufyaan's Website

sufyaan.me/tfa

# Start Using 2FA Properly

**13 May 2023**

**Category:** Software & Guides

If you use any online account, you should use 2FA keys. It does not matter if it is your Google account that has all of your personal information or if it is some random account you use once in a while. You should at least have 2FA enabled in an authenticator app or preferably a 2FA key. Do not use SMS.

Why buy a 2FA key when you can use 2FA codes or SMS for free? Let us start with SMS.

## SMS

SMS is inherently insecure. It is not encrypted, and your SIM card is always susceptible to SIM swap attacks. A SIM swap attack is a type of identity theft where a cybercriminal pretends to be you and asks for your number to be switched to a SIM card in their possession. They do this by claiming that their phone was lost or stolen. Most employees working for mobile networks speak with hundreds of people a day. They cannot differentiate people's voices. Even with a small amount of voice modulation, almost anyone can trick them into thinking it's you.

After gaining possession of your SIM card, the cybercriminal goes to your online accounts and tries to reset your passwords. If they already have your passwords, they may try to login using your phone number and the 2FA code received through SMS. This may seem rare, and it may also seem like it does not work on most people. However, in 2019, Jack Dorsey's (the former CEO of Twitter) account got hacked using this exact method.

As commonly said by many privacy and security professionals, you are only as secure as your weakest link. Make sure your weakest link is not SMS.

## Authenticator Apps

An authenticator app is much better than SMS-based 2FA. This is because authenticator apps usually follow the TOTP or HOTP standard, which is very secure. It basically uses a secret key along with the current time to create a unique code that changes every thirty seconds.

One thing that you should absolutely not do is use Google Authenticator, Microsoft Authenticator, Authy or anything as such. This is because the clients are close-sourced, which means that the code is not public. This means that they could be doing anything with your 2FA secret keys. Authy syncs your codes which is convenient but it does not allow you to export your keys, just like other properietary authentication apps. This is unethical as you should have complete control over what is required to access your own accounts. If your Authy account gets disabled, you will no longer be able to log in to most accounts. A much better alternative is:

- Aegis (Android)
- Raivo (iOS)
- Tofu (iOS)
- password store with pass-otp (UNIX-based systems)
- Keepass Password Manager (Linux/Windows/MacOS/Android/iOS)

You should also be taking frequent **encrypted backups** of not only your 2FA codes, but all data that is important to you. Read this post to learn how to take encrypted backups properly. Remember, you should

keep your backups as far away from other people's hands as possible. If they have your secret keys, they have your 2FA codes.

## Security Keys

Security keys are the best form of two-factor authentication. They are physical keys which need to be plugged in to your computer or smartphone in order to be used. They use NFC, USB-C, USB-A and also the Lightning port. This 2FA method makes it so that it does not matter which person gets your credentials because they need access to your key physically in order to login. One drawback of this method is that, if you lose your key, you cannot login to your accounts. This is why people buy 2 or 3 as a backup. It should be noted that, although other methods can be used alongside security keys, it is not recommended as it is still possible to just use the other insecure methods for a cybercriminal and bypass your security key.

I recommend Yubico and NitroKey security keys.

## Conclusion

If there is one thing you take away from this post, it is to make 2FA your baseline security protocol. Use 2FA for **every account that has it.** Do not use SMS, use authenticator apps. If possible, spend money on three security keys.