

Forum:[Hack Forums](#)

Thread: [Is it possible to bypass 2fa \(authy \)?](#)

Justin Bieber - February 15, 2017, 11:37 am

Hello, I just want to activate 2fa on facebook through authy. before activating that, I want to know that; if my account gets leaked and someone enter in it, is it possible to bypass 2fa? or he gets fucked and my account is safe?

Please let me know that. I don't wanna activate something asking a code everytime I log in (very boring) when it could be hacked.

Better authy or sms code?

Thank you

__ZZ - February 15, 2017, 11:51 am

If he manages to break through your phone and make you download a RAT onto your phone, he might be able to access your messages and read them which gives him the ability to find the 2fa auth code you would get when logging into FB. So that's the only way I know how to bypass 2fa. If anybody knows another way please share your thought. Good luck OP.

Flared - February 15, 2017, 11:53 am

Only way to bypass 2fa is to get to the source. Whether it be an email or phone #

Phobiya - February 15, 2017, 3:39 pm

tbh bro its a waste on time putting two step on any social medium... just use a email thats long and only for that account with a generated password written down irl...

Exquisite. - February 15, 2017, 3:39 pm

No. Plus, it defeats the purpose of 2FA

suffixor - February 15, 2017, 10:25 pm

No there is no way.

The way these services work is through the TOTP algorithm.

https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm

What happens is, facebook generates a long random secret which is transferred to the authy app usually through a QR code or by typing it in.

Your phone then hashes this secret through with the time every 30 seconds.

You then use this hash to generate an n digit number. You enter this number into facebook, facebook hashes the time with the secret key to generate a token, if the token matches the one you enter it logs you in.

To bypass this, you would either need to steal the TOTP secret by hacking facebook or by hacking/stealing the phone, or by hacking authy.

Authy is better than SMS because it's reliant on secure crypto and not the social engineering resistance of your phone carrier.

Poutine - February 15, 2017, 10:25 pm

Take a look at smishing attack.

?Criminal - February 17, 2017, 5:10 pm

Authy can be bypassed due to a built in fallback mechanism not only have I bypassed it before but a few friends have as well, the only secure TOTP would be gauth you need physical access to the phone or to somehow get the token before it expires which is seconds I believe which can be done with a quick SE or malware on the device like the person a bit above stated.