

### SMS-2FA is harmful and literally doesn't work. There is no reason to ever enable it.

**Seth Hall** @loteck · Mar 15, 2021  
Another day, another chance to remind everyone that text-message passwords are not multi-factor authentication, it's two-step verification using only 1 factor. "SMS 2FA" is an oxymoron & harmful for MFA efforts. CCing my fave opinionites @riskybusiness @Metlstorm @tavis twitter.com/josephcox/sta...

7:47 PM · Mar 15, 2021 · Twitter Web App

127 Retweets 23 Quote Tweets 346 Likes

Reply Retweet Like Share icons

**Dani Cela** @dani190 · Mar 15, 2021  
Replying to @tavis  
What's the recommendation of a company offers no alternatives? Is no 2fa better in that case?

**Seth Hall** @loteck · Mar 15, 2021  
Not speaking for him, but I do remember Tavis advised simply using good, unique passwords if you can't MFA. [blog.cmpxchg8b.com/2020/07/you-do](http://blog.cmpxchg8b.com/2020/07/you-do)

**Josh Bressers** @joshbressers · Mar 15, 2021  
Replying to @tavis  
That story is horrifying


**FIPSmode Squad** @anthonypants · Mar 15, 2021  
Replying to @tavis  
it works very well at collecting cell phone numbers from customers that they might not otherwise share :)

**Richard Johnson** @richinseattle · Mar 15, 2021  
Replying to @tavis  
Your banks offer something better?

**Tavis Ormandy** @tavis · Mar 15, 2021  
The only possible attack that SMS-2FA has any impact on at all is credential stuffing, and it's a crappy solution. We have a really good solution that doesn't require your bank to do anything, unique passwords... so yes 😊

**TerrenceDeterrence** @TerrenceDeterr1 · Mar 15, 2021  
Replying to @tavis  
Wait, it's a (smallish) barrier if you are using the phone to authenticate transactions made on another device. If device is compromised but phone isn't, attackers cannot initiate transactions. If sms contains transaction details, it may also stop transaction modification.

**Herbert Bos** @herbertbos · Mar 18, 2021  
I agree. It's very weak, but the effect is not zero. (Otoh: it is indeed trivial to intercept sms. You don't need fancy ss7 attack either. Perhaps the bandroid vulnerability still works even, as Google did not want to fix it.)

 vusec.net  
**BAndroid - VUSec**  
Project Description The BAndroid vulnerability allows an attacker with control over your browser to also take control over your mobile phone. In broad strokes, the scenario is as follows. If attack...

This Tweet was deleted by the Tweet author. [Learn more](#)

**Tavis Ormandy** @tavis · Mar 15, 2021  
No, it doesn't mitigate those attacks. That's the problem, if it did then that would be great.  
"Don't let the perfect be the enemy of the good" only applies when something is good enough, but not perfect. The problem is that SMS-2FA is \*not\* good enough.

Show replies

