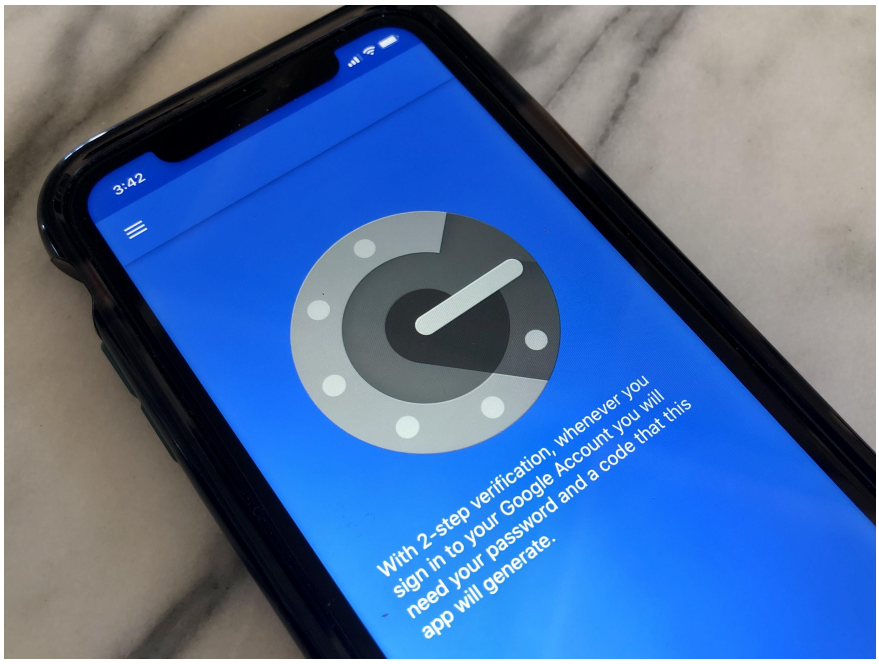
Do you use SMS for two-factor authentication? Don't.

The coronavirus pandemic has lead to a rise in hackers and scammers preying on people's fears during these turbulent times, from SIM swapping to phishing scams meant to look like stimulus check emails.

You would be wise to be on the lookout for coronavirus scams, and you'd be even wiser to use two-factor authentication to protect your personal information and online accounts. And if you are using two-factor authentication, you'd be wiser still to use an authentication app rather than receiving codes through text, also known as SMS.



Using an authentication app is a win-win. Not only is it more secure than getting codes texted to you, but it also makes the login process faster. Time for a quick Q&A:

Wait, what is two-factor authentication?

Two-factor authentication (2FA) -- also known as two-step verification or multifactor authentication -- adds a layer of security to your online accounts, from Amazon, Apple and Google to Facebook, Instagram and Twitter. Instead of entering only your password to access an account, you need to enter your password -- the first verification factor -- and then a code sent via SMS or a prompt through an authentication app -- the second factor. This means a hacker would need to steal both your password and your phone to break into your account.

So, why the move away from SMS?

For the simple fact that receiving 2FA codes via SMS is less secure than using an authentication app. Hackers have been able to trick carriers into porting a phone number to a new device in a move called a SIM swap. It could be as easy as knowing your phone number and the last four digits of your Social Security number, data that tends to get leaked from time to time from banks and large corporations. Once a hacker has redirected your phone number, they no longer need your physical phone in order to gain access to your 2FA codes.

Also, if you sync text messages with your laptop or tablet, then a hacker could gain access to SMS codes by walking off with such a device of yours.

Then there are the weaknesses in the mobile telecom system itself. In what's called an SS7 attack, a hacker can spy via the cell phone system, listening to calls, intercepting text messages and seeing the location of your phone.

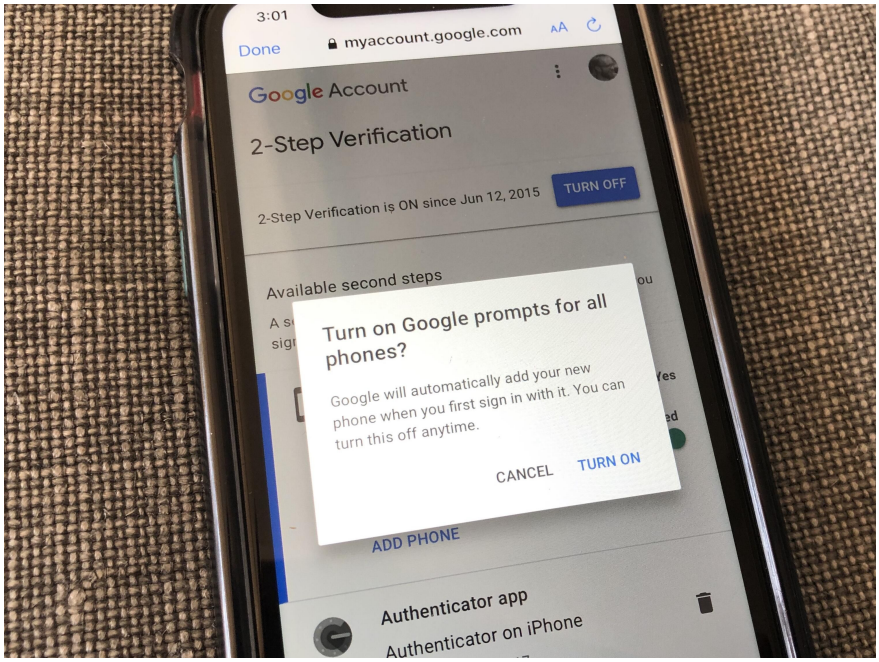
All of the above scenarios are bad news for those receiving 2FA codes via SMS.

What should I use instead?

An authentication app such as Google Authenticator, Microsoft Authenticator or Authy. It has the advantage of not needing to rely on your carrier; codes stay with the app even if a hacker manages to move your number to a new phone. And codes expire quickly, usually after 30 seconds or so. In addition to being more secure than SMS, an authentication app is faster; you need only to tap a button to verify your identity instead of manually entering a six-digit code.

If you have an Android phone or an iPhone with the Google Search or Gmail app, you can set up Google prompts to receive codes without needing a separate authentication app. You'll receive 2FA prompts as push notifications on your phone that require a simple tap to approve.

Picture 2 of Do you use SMS for two-factor authentication? Don't.



Do I even need two-factor authentication if SMS is so vulnerable?

Yes! In addition to creating strong passwords and using different passwords for each of your accounts, setting up 2FA is the best move you can make to secure your online accounts -- even if you insist on receiving codes via SMS. Two-step verification via SMS is better than one-step verification where a hacker needs only to obtain or guess your password in order to gain access to your data. Don't be the low-hanging fruit with an account that is the easiest target for hackers.

But two-factor authentication is a hassle

That's not a question, but my counter would be that it's less of a hassle when done right and you are receiving codes via Google prompts or an authentication app where you don't need to enter six-digit codes. Sure, even then it does force you to take an extra step of grabbing and tapping your phone after entering your password to log into one of your accounts. I would argue, however, that the hassle of the second step of two-factor authentication pales in comparison to the hassle of getting hacked. At best, getting hacked is a hassle. More often, it's a mix of anger, pain, loss and confusion.

For more ways to keep safe and stay secure, here's how to improve your Zoom security to prevent Zoombombing, the guide to password security (and why you should care), how to secure your Amazon account and how to secure your Gmail account.