Receiving a login code via SMS and email isn't secure. Here's what to use instead

March 6 2019, by Mike Johnstone

Credit: AI-generated image (disclaimer)

When it comes to personal cybersecurity, you might think you're doing all right. Maybe you've got multi-factor authentication set up on your phone so that you have to enter a code sent to you by SMS before you can log in to your email or bank account from a new device.

What you might not realise is that new scams have made authentication using a code sent by SMS messages, emails or voice calls less secure than they used to be.

Multi-factor authentication is listed in the Australian Cyber Security Centre's Essential Eight Maturity Model as a recommended security measure for businesses to reduce their risk of cyber attack.

Last month, in an updated list, authentication via SMS messages, emails or voice calls was downgraded, indicating they're no longer considered optimal for security.

Here's what you should do instead.

What is multi-factor authentication?

Whenever we log in to an app or device, we are usually asked for some form of identity check. This is often something we know (like a password), but it can also be something we have (like a security key or an access card) or something we are (like a fingerprint).

The last of these is often preferred because, while you can forget a password or a card, your biometric signature is always with you.

Multi-factor authentication is when more than one identity check is conducted via different channels. For instance, it's common these days to enter your password, and an extra authentication code you need to enter is sent to your phone via SMS message, email or voice mail.

Lots of services, such as banks, already offer this feature. You're sent a "one-time" code to your phone in order to confirm authority to enact a transaction.

This is good because:

- it uses two separate channels
- the code is randomly generated, so it can't be guessed
- the code has a limited lifetime

How could this go wrong?

Suppose a cybercriminal has stolen your phone, but you have it locked via fingerprint. If the criminal wants to compromise your bank account and attempts to log in, your bank sends an authentication code to your phone.

Depending on how your phone settings are configured, the code could pop-up on your phone screen, even when it's still locked. The criminal could then input the code and access your bank account. Note that "do not disturb" settings on your phone won't help as the message still appears, albeit quietly. In order to avoid this problem, you need to disable message previews entirely in your phone's settings.

A more elaborate hack involves "SIM swapping". If a criminal has some of your identity details, they might be able to convince your phone provider that they are you and request a new SIM attached to your phone number to be sent to them. That way, any time an authentication code is sent from one of your accounts, it will go to the hacker instead of you.

This happened to a technology journalist in the US a couple of years ago, who described the experience: "At about 9pm on Tuesday, August 22 a hacker swapped his or her own SIM card with mine, presumably by calling T-Mobile. This, in turn, shut off network services to my phone and, moments later, allowed the hacker to change most of my Gmail passwords, my Facebook password, and text on my behalf. All of the two-factor notifications went, by default, to my phone number so I received none of them and in about two minutes I was locked out of my digital life."

Then there is the question of whether you want to provide your phone number to the service you are using. Facebook has come under fire in recent days for requiring users to provide their phone number to secure their accounts, but then allowing others to search for their profile via their phone number. They have also reportedly used phone numbers to target users with ads.

This is not to say that splitting identity checks is a bad thing, it's just that sending part of an identity check via a less-secure channel promotes a false sense of security that could be worse than using no security at all.

Multi-factor authentication is important – as long as you do it via the right channels.

Which authentication combinations are best?

Let's consider some combinations of multi-factor authentication that have varying degrees of ease of use and security.

An obvious first choice is something you know and something you have, say a password and a physical access card. A cybercriminal has to obtain both to impersonate you. Not impossible, but difficult.

Another combination is a password and a voiceprint. A voiceprint recognition system records you speaking a particular passphrase and then matches your voice when you need to authenticate your identity. This is attractive because you can't leave your voice at home or in the car.

But could your voice be forged? With the aid of digital software, it might be possible to take an existing recording of your voice, unpack and re-sequence it to produce the required phrase. This is somewhat challenging, but not impossible.

A third combination is a card and a voiceprint. This choice removes the need to remember a password, which could be stolen, and as long as you keep the physical token (the card or key) safe, it is very hard for someone else to impersonate you.

There are no perfect solutions yet and using the most secure version of authentication depends on it being offered by the service you are using, such as your bank.

Cyber security is about managing risk, so which combination of multi-factor authentication suits your needs depends on the balance you accept between usability and security.

Provided by The Conversation

Citation: Receiving a login code via SMS and email isn't secure. Here's what to use instead (2019, March 6) retrieved 9 April 2024 from https://phys.org/news/2019-03-login-code-sms-email-isnt.html