Can I still be hacked with 2FA enabled?

4 September 2020, by David Tuffley

Credit: Shutterstock

Cybersecurity is like a game of whack-a-mole. As soon as the good guys put a stop to one type of attack, another pops up.

Usernames and passwords were once good enough to keep an account secure. But before long, cybercriminals figured out how to get around this.

Often they'll use "brute force attacks", bombarding a user's account with various password and login combinations in a bid to guess the correct one.

To deal with such attacks, a second layer of security was added in an approach known as two-factor authentication, or 2FA. It's widespread now, but does 2FA also leave room for loopholes cybercriminals can exploit?

2FA via text message

There are various types of 2FA. The most common method is to be sent a single-use code as an SMS message to your phone, which you then enter following a prompt from the website or service you're trying to access.

Most of us are familiar with this method as it's favored by major social media platforms. However, while it may seem safe enough, it isn't necessarily.

Hackers have been known to trick mobile phone carriers (such as Telstra or Optus) into transferring a victim's phone number to their own phone.

Pretending to be the intended victim, the hacker contacts the carrier with a story about losing their phone, requesting a new SIM with the victim's number to be sent to them. Any authentication code sent to that number then goes directly to the hacker, granting them access to the victim's accounts.

This method is called SIM swapping. It's probably the easiest of several types of scams that can circumvent 2FA.

And while carriers' verification processes for SIM requests are improving, a competent trickster can talk their way around them.

Authenticator apps

The authenticator method is more secure than 2FA via text message. It works on a principle known as TOTP, or "time-based one-time password."

TOTP is more secure than SMS because a code is generated on your device rather than being sent across the network, where it might be intercepted.

The authenticator method uses apps such as Google Authenticator, LastPass, 1Password, Microsoft Authenticator, Authy and Yubico.

However, while it's safer than 2FA via SMS, there have been reports of hackers stealing authentication codes from Android smartphones. They do this by tricking the user into installing malware (software designed to cause harm) that copies and sends the codes to the hacker.

The Android operating system is easier to hack than the iPhone iOS. Apple's iOS is proprietary, while Android is open-source, making it easier to install malware on.

2FA using details unique to you

Biometric methods are another form of 2FA. These include fingerprint login, face recognition, retinal or iris scans, and voice recognition. Biometric identification is becoming popular for its ease of use.

Most smartphones today can be unlocked by placing a finger on the scanner or letting the camera scan your face—much quicker than entering a password or passcode.

However, biometric data can be hacked, too, either from the servers where they are stored or from the software that processes the data.

One case in point is last year's Biostar 2 data breach in which nearly 28 million biometric records were hacked. BioStar 2 is a security system that uses facial recognition and fingerprinting technology to help organizations secure access to buildings.

There can also be false negatives and false positives in biometric recognition. Dirt on the fingerprint reader or on the person's finger can lead to false negatives. Also, faces can sometimes be similar enough to fool facial recognition systems.

Another type of 2FA comes in the form of personal security questions such as "what city did your parents meet in?" or "what was your first pet's name?"

Only the most determined and resourceful hacker will be able to find answers to these questions. It's unlikely, but still possible, especially as more of us adopt public online profiles.

2FA remains best practice

Despite all of the above, the biggest vulnerability to being hacked is still the human factor. Successful hackers have a bewildering array of psychological tricks in their arsenal.

A cyber attack could come as a polite request, a scary warning, a message ostensibly from a friend or colleague, or an intriguing "clickbait" link in an email.

The best way to protect yourself from hackers is to develop a healthy amount of skepticism. If you carefully check websites and links before clicking through and also use 2FA, the chances of being hacked become vanishingly small.

The bottom line is that 2FA is effective at keeping your accounts safe. However, try to avoid the less secure SMS method when given the option.

Just as burglars in the real world focus on houses with poor security, hackers on the internet look for weaknesses.

And while any security measure can be overcome with enough effort, a hacker won't make that investment unless they stand to gain something of greater value.

APA citation: Can I still be hacked with 2FA enabled? (2020, September 4) retrieved 23 October 2021 from https://techxplore.com/news/2020-09-hacked-2fa-enabled.html