What is multi-factor authentication

Jongkil Jay Jeong, *Deakin University*; Ashish Nanda, *Deakin University*, and Syed Wajid Ali Shah, *Deakin University*

Data breaches are becoming commonplace in both small and big tech companies. The most recent victim was Australian telecommunications company Optus, resulting in unauthorised access to the identity data of roughly 10 million people.

Adding to the misery of the victims, this cyber-attack further unleashed a plethora of subsequent phishing and fraud attempts using the data obtained from this breach.

Having more rigorous security measures when logging in can help to protect your accounts, and significantly reduces the likelihood of many automated cyber attacks.

Multi-factor authentication (MFA) is a security measure that requires the user to provide *two* (also known as two-step verification or two-step authentication) or more proofs of identity to gain access to digital services. This typically requires a combination of something the user knows (pin, secret question), something you have (card, token) or something you are (fingerprint or other biometric).

For example, the Australian Tax Office recently tightened some rules for digital service providers on the mandated use of multi-factor authentication. If you use certain services, you're already familiar with MFA.

But not all MFA solutions are the same, with recent studies demonstrating simple ways to subvert more common methods which are used to lodge cyber-attacks.

Furthermore, people also prefer different MFA options depending on their needs and level of tech savviness.

So what are the options currently available, their pros and cons, and who are they suited for?

There are four main methods of multi-factor authentication

- **SMS**: Currently the most common option involving a one-time password (such as a code) sent via text message. Although quite popular and easy to use, the password or code texted to you can commonly be hacked by malicious apps on the phone or by redirecting the SMS to a different phone. The method also fails if your smartphone doesn't have service or is powered off.
- **Authenticator-based**: Another common method, in which an application installed on your smartphone (such as Google Authenticator) generates one-time passwords valid for a very short time span, such as 30 seconds. Although more secure than text messages, malicious apps can still steal these one-time passwords. The method also fails if your smartphone is out of power.
- **Mobile app**: Similar to authenticator apps, but a user is sent a verification prompt rather than a one-time password. This requires your smartphone to have an active internet connection and be powered on.
- **Physical security key**: The most secure mechanism; it uses a hardware security key (such as YubiKey, VeriMark or Feitian FIDO) that needs to be connected to the device to verify identity – many of these look a lot like USB memory sticks. It's the current leading method supported by companies like Google, Amazon and Microsoft, as well as government agencies worldwide.

Each of these four methods varies in usability and security. For example, despite physical security keys offering the greatest level of security, the adoption rate is the lowest, with figures suggesting only a 10% uptake.

Preference matters

Not only do different multi-factor authentication types vary in security, they also have different levels of popularity. This results in a discrepancy between the most *reliable* MFA method (the physical security key) and what is actually the most *widely used* (SMS).

Our team from Deakin University's Centre for Cyber Security Research and Innovation recently conducted a study on the adoption of MFA technologies. We surveyed more than 400 participants belonging to different age groups, educational backgrounds, and experience with MFA.

Results from our study indicate that people's preferences are impacted not just by their security needs, but also by usability. The majority of users cared most about the *simplicity* of the MFA method – this clearly explains why SMS-based solutions still dominate the landscape, even though there are safer alternatives.

In our follow-up study, users were given the most popular physical security keys for one month, to test unsupervised. Preliminary results suggest most users found the physical keys effective and intuitive to use.

However, the lack of platform support and setup instructions created a *perception* that these keys were difficult and complex to install and use, resulting in a lack of willingness to adopt.

One size does not fit all

We believe there needs to be careful consideration before any government agency or company mandates MFA, with a few key steps to consider.

Different people and organisations will have different needs, so in some cases a combination of methods could work best. For example, an SMS-based solution may be used in conjunction with a physical security key for access to critical infrastructure systems that need higher levels of security.

Additionally, user education and awareness is vital. Many people aren't aware of the importance of MFA, and don't know which methods are the safest.

By taking some personal responsibility and using highly effective methods such as physical security keys to protect our most vulnerable accounts, we can all do our part to make the web a safer place.

Jongkil Jay Jeong, CyberCRC Senior Research Fellow, Centre for Cyber Security Research and Innovation (CSRI), *Deakin University*; Ashish Nanda, CyberCRC Research Fellow, Centre for Cyber Security Research and Innovation (CSRI), *Deakin University*, and Syed Wajid Ali Shah, CSCRC Research Fellow, Centre for Cyber Security Research and Innovation, *Deakin University*