28 AUGUST 2020
WMCYBER@WEST-MIDLANDS.PNN.POLICE.UK
WWW.WMCYBER.ORG

West Midlands | Regional Cyber Crime Unit

Multi-factor or Two Factor Authentication (2FA)

What is Multi-factor or Two Factor Authentication (2FA)?

With regular developments in technology, humans have had to develop new ways to authenticate people they don't directly know. In the physical environment, we often authenticate by looking at someone and/or their physical ID. In the virtual environment, something called multi-factor or, more commonly, two factor authentication (2FA) has been developed as an extra layer of security for online activity. MFA provides a way of 'double checking' who you really are when using online services, such as banking, email or social media.

How do we use 2FA and what types of authentication are available?

We have been using 2FA for years; when you put a debit card (something you have) into an ATM, it needs a pin (something you know). The most common MFA is 2FA; a text message is sent to a mobile phone, while using a bank/credit card online, which is entered to authorise the transaction. This also has a time limit for using the code, to prevent fraudsters using the same code later.

Location is one layer and organisations may limit access to data to those from within a secure network or by a specific device. A GPS derived location from a smartphone or IP address may also be used to limit access. Some media sites use this to limit programmes broadcast by geographic region.

Other layers of authentication may be time based - only allowing access to users at certain designated times. Banks may use time and location for checking withdrawals - it's impossible to withdraw from an ATM in London and 45 minutes later from an ATM in Glasgow.

Biometric authentication is another layer – facial recognition, fingerprint, voice recognition and retinal scan. By applying multiple variations of these factors it is possible to greatly increase the security of systems and data accessed.

How to set up 2FA?

When setting up 2FA, the service will ask for a 'second factor', which is something that you (and only you) can access - a code sent by text message or created by an app.

- Text or Voice messages - During setup, provide the phone number, and the service will send a code to use. Some services also offer sending a code using a voice message.
- Authenticator Apps on a smart phone (or tablet) are the main alternative to text messages. Google Authenticator and Microsoft Authenticator are examples. Apps offer advantages, such as not needing a mobile signal, or waiting for a text message to arrive. The option to switch on MFA is usually found in security settings, it may be called 'two-step verification'.

For more information visit the NCSC's guidance on multi-factor authentication visit:
Multi-factor authentication for online services – https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services
Setting up two-factor authentication (2FA)
https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa
Turn on two-factor authentication – Social Media, Banking & Email
https://www.ncsc.gov.uk/cyberaware/home#section_4

Additional Top tips

Use MFA when online, as it significantly reduces the risk of fraud.

- The website www.telesign.com/turnon2fa/tutorials also contains up-to-date instructions on how to set up 2FA across popular online services such as Gmail, Facebook, Twitter, LinkedIn, Outlook and iTunes.
- Do not to publicise your mobile phone number on social networking sites and if your phone line goes down, contact your service provided immediately.