Queensland Law Society

Cybersecurity

Multi Factor Authentication Guide

Version 2.1 January 2023

MULTI FACTOR AUTHENTICATION ('MFA')

Snapshot

Passwords can be easily stolen or forced in a number of ways, and this is the most common way a law firm is attacked. If a single password is all that stands between criminals and your client's data and money, your firm is at significant risk.

There are three keys to reducing this vulnerability:

1. Making your passwords more secure, using a combination of policies, training and systems.[1]
2. Using Multi Factor Authentication ('MFA') to add a second barrier between critical data and the attacker.
3. Ensuring your procedures acknowledge the inherent insecurity of email and that email messages are not treated as a source of truth for large financial transactions.

All of these approaches complement each other and using them together is important. No matter how careful an organisation is, eventually someone will slip up and a password will be lost. If the criminal also needs a second means of identification to access records or funds, the chances of both methods of verification being compromised at once are much lower.

Many of your online accounts probably already have this feature, and all you need to do is turn it on. The Lexon Cyber Protocol requires firms to use MFA to protect critical accounts, such as email and practice management software.

Key point: Using Multi Factor Authentication is a very cost-effective way to make your data and bank accounts more secure. It is not perfect, but any organisation which takes confidentiality seriously will *use it* where possible.

How does MFA work?

There are a number of different options. The basic idea is that after a password is entered, a user is asked to provide further proof of identity. The most common variants are:

- A single-use number ("One Time Pass: OTP") sent to you by SMS (not recommended);
- Biometric options such as fingerprint or retina (fairly secure, but you need to be sure the verification is done on your phone / device and not sent off to a remote database);
- An OTP generated by an App (better);
- Push authorisation (good, but not as reliable); and
- A physical key or device that shows a continuously updating OTP, or is inserted / contacts your device over a short distance (currently the most secure option).

The App used to generate codes can come from a variety of sources. Google and Microsoft offer high quality, free options that are compatible with nearly any MFA system. The function may also be built into a provider's App (your bank, for example).

Obviously, any device used to retrieve MFA codes should also be protected.

Key point: Many online accounts offer a variety of MFA options. Any of them is *much better than nothing.* Some are better than others.

[1] Note that if your firm undertakes electronic conveyancing, both PEXA and Sympli users have mandatory password and security requirements. These requirements and other compliance materials can be found in the electronic conveyancing security toolkit available on the QLS website.

A quick guide of the basic MFA options

SMS: Pros and Cons

Pin codes delivered by SMS are offered by most MFA systems. These are reliable and easy to explain. However, SMS was never intended to be highly secure; a determined attacker might get control of a user's phone as a stepping stone to their email and bank accounts.

The two main ways to do this are by tricking your phone provider into transferring the mobile number to the attacker (which is often much easier than it should be) or by using technical vulnerabilities in the phone network.

Despite this, MFA supplied by SMS is still more secure than not using anything at all, and if that is the *only* option offered, you should use it (however, it is important to check back every so often to see if the options have been expanded). Note: using SMS to receive second factor codes does not satisfy the Lexon Cyber Protocol (2023 version).

Biometrics: Pros and Cons

Biometric authentication such as fingerprint, facial recognition or retina scans are increasingly popular, especially on mobile devices. They can be circumvented as well, but not easily. Biometric scans are convenient and are becoming increasingly reliable.[2]

The problem with using biometrics is that they all rely upon scanning an essential human feature and turning it into a digital sequence. If that sequence is then transmitted across a network, there is the chance of that being intercepted. Once a digitized fingerprint (retina / voiceprint) is lost you have a real problem because you can't change it in the same way you can change a password.

Not all biometric systems work this way, and most don't send your digitized information anywhere, but analysing that risk is a job for an expert.

Authenticator App: Pros and Cons

Google (Google Authenticator) and Microsoft (Microsoft Authenticator) provide free "one time code" generating apps. They are widely used and should be compatible with most services offering MFA. Several other providers supply this service as well.[3]

When you want to log into the service you consult the authenticator and read the appropriate six digit number. This number is inserted into your service to complete the log in process. Each number only lasts 30 - 60 seconds before it expires and a new one is generated.

As at 2022/23 an authenticator app is probably the best choice for enabling MFA in an organisation without full time IT support.

Push Authorisation: Pros and Cons

Some websites (Google accounts, for example) can send a request to your phone asking for confirmation before a log in is completed. If the person in possession of the device clicks 'yes', you can proceed. The authorisation system uses either an authentication app installed on the phone or a native function built into the operating system (such as Apple).

Push Authorisation is more secure and slightly more convenient than SMS or an authenticator app code that you manually enter.

---

[2] There have been some notable failures: the Samsung Galaxy s10, for example, where the addition of a $2 silicon phone cover would allow any fingerprint to access the device. (Story here (third party link))

[3] For a rated list see: here (third party link)

It is harder[4] to intercept and re-use push authentication, however the difference is only moderate. When push notification stops working it can be frustrating, and is often a problem with the user's phone settings so it can be hard for an IT support desk to troubleshoot.

Key / Dongle: Pros and Cons

A key is a physical device that works a little like a house key. When prompted, the user plugs the key into the laptop / phone or presses a button which transmits the code. In some cases, the key will ask you to apply a fingerprint or enter a pin number. The two most common brands are Google's Titan Key or a Yubico key. Large institutions might have a similar proprietary system either built into staff ID/building access cards or as a stand-alone device (such as the PEXA digital signature token).

From a security perspective, a key is the gold standard for MFA systems – especially where it requires a fingerprint/pin to use it.

It is more complicated and expensive to set up than the other options and is not as universally compatible with common cloud services or software.

Key point: Unless you have especially sensitive data to protect, use of an Authenticator app *is a sound choice in 2022/23*, but you should consider upgrading to a physical key eventually.

Other choices an MFA system may offer

Some MFA systems allow you to turn features on and off – usually balancing security with convenience. An example might be whether you need a code every time, only once in a while or when connecting a new device. Choosing 'maximum safety' every time might not be the best course, especially if you annoy your staff so much that they turn the feature off altogether.

Consider how critical the system is. What is a reasonable choice for the firm Facebook account may not be adequate for email accounts, for example.

What should I protect using MFA?

In short, as much as you can. The following should definitely be protected:

- Servers and remote access to your office computers[5]
- All cloud storage
- All email (even free email, especially if you can use it to reset other passwords).[6]
- Office 365 / GSuite or equivalent
- Banking
- E-conveyancing and transaction platforms
- HR / Payroll / Staff records portals
- Practice Management Systems
- Social Media[7]
- Court and government portals
- Your own website (if available).

Training and user acceptance

Most MFA systems work quite well, but it is still slightly less convenient than just putting in a password.

[4] But not, unfortunately, impossible.
[5] Even better, turn remote access off!
[6] It is quite common to set up a free email account for one purpose and then use it for more than was intended.
[7] Hacked social media accounts can create reputational damage and also be used to spread malware to clients and colleagues.

If staff understand why they are being asked to take extra steps, they are more likely to cooperate. The fewer teething problems the better – if a system fails the first few times, people may not trust it even if the problems are easily fixed.

A simple three step process can save time in the long run:

1. Select, deploy and test the new system. Ensure it works well before going live.
2. Adopt a policy mandating use of the process.
3. Train all staff on:
    - why the change is required;
    - some case studies (if available);
    - what the policy is, and how to ask any questions or adapt it to their own work group;
    - how to use the solution, and how to get help if they get stuck.

Get feedback, audit and verify compliance. The initial reminders should be fairly gentle, but make it plain that future noncompliance will have consequences.

Training can be short and to the point, but sending an email is usually insufficient. Ideally, the training session should be backed with reminders, such as emails, posters in common areas and laminated 'how to' cards to be attached to computer monitors.

How do I turn on MFA?

In most cases it is pretty simple. If you check the cloud or service provider's website, the answer can often be found quickly. If they have a customer support team, they will usually be happy to point you in the right direction.

If you can have IT support available for a few hours during the implementation this can assist users who are encountering problems to get started. This may reduce frustration and increase user acceptance.

One point to note is that MFA is usually not turned on by default, so even if the vendor refers to it in the sales process you will usually have to take an extra step to enable it. In some cases you may require an additional license, which is irritating but still worth it.

Make it clear to your IT team that your default position is that MFA should be enabled and ask them to talk to you first if they decide to turn it off for any reason.

If you don't have in-house IT support, it is well within the DIY capabilities of many people.

Setting up the authenticator apps is usually fairly straightforward. In general terms:

- Download Google or Microsoft Authenticator app(s) on your phone.
- Go to the website service you want to protect and navigate to account or security settings.
- Activate MFA and select the authenticator app you are using.
- You will usually get a code (or a QR code) to put into the authenticator to link the two accounts.

So, I have done all that and my network must be secure, right?

Unfortunately not. There are a number of ways around MFA systems so they must be regarded as a security layer not an impregnable defence. The main ways to circumvent MFA are:

Risk	What to do about it.
Phishing. An impersonator pretends to be from the bank / an IT provider and walks your staff member through a "log in". When the OTP code is issued, the staff member supplies it to the attacker.	Ensure staff know not to input passwords when following links. Eg. "your bank account is being accessed, protect it here" Ensure staff know not to follow links to critical sites in the first place.
Fake website. A criminal sets up a fake website to look like a bank or transaction platform. They take out a Google Ad so a search reveals the	Links to all critical accounts should be saved on the desktop, rather than Google-searching the (eg.) bank website each time.

fake site. Users can't log in, but there is a convenient "help here" button that puts you in touch with a friendly person to whom you give your username, password and one time code. An even more sophisticated version cuts the person out of the loop and automates the attack.	Turn off Autofill in your web browser (Instructions: How to turn off Autofill (third party link) Turn off SMS verification code autofill for your Apple or Android device
Browser attack. (MITTM attack) Sophisticated malware can take control of your browser showing one thing on the screen and doing something else behind it (eg. screen shows transferring $100 from trust to person x, browser instructs transferring $1000 from trust to person y. When the bank issues the OTP the user inputs it, authorising the second transaction not the first one as intended).	Ensure operating systems and browsers are kept up to date. Install quality third party virus protection. Discuss protections with your IT advisor such as virtualization and sandboxing for high risk machines (the people that do your internet banking, for example).

Further resources can be found here:

- A guide to common types of Two-Factor Authentication
- Office 365 MFA Guide
- Leap Two-Factor Authentication (2FA) guide
- PEXA MFA

QLS Cyber Essentials Insurance
FREE for member practices with Lexon PI insurance • **qls.com.au/cyber**