TFA via Authenticator App – an explanation

Secure websites use mandatory Two Factor Authentication (TFA) to VERIFY THE IDENTITY OF USERS who have access to secure areas and therefore access to private and sensitive data. TFA adds an extra layer of security that makes it significantly harder for someone to access an account - and therefore the secure area - even if they have managed to acquire a user's password.

Undertaking TFA via an 'authenticator' app is more secure than having a passcode sent via email. For this reason, TFA by alternate email is no longer supported by the AISWA website. Many banks and businesses already require the use of a generic or bespoke identity authentication app.

What does an authenticator app do?

An AUTHENTICATOR APP generates a RANDOM ONE-TIME PASSCODE that is used to confirm your identity when logging into a secure online service. It is a second line of defence after your username and password.

An authenticator app is downloaded and installed on your mobile device. The mobile device most often used is a phone – but other mobile devices such as iPads and Apple Watches can also accommodate authenticator apps. Check the app store on your preferred device and follow the download and installation instructions.

Watch a simple explanation of authenticator app services here.

Here is the list of authenticator apps that will work with the AISWA website. Links to generic *YouTube* explanations are included to help you choose. Search your app store to find and download your chosen app.

.

- Google Authenticator (Android/iPhone)
- Microsoft Authenticator (Android/iPhone).
- Authy (Android/iPhone/desktop version)
- FreeOTP (Android, open source)

What happens in the initial set-up?

This 'set-up' process is done ONCE ONLY to establish an INITIAL CONNECTION between the website and the authenticator app on your device.

When you first set up an authenticator app for a secure online service (the AISWA website), the service being accessed (the AISWA website) generates a 'key'. This is a unique random collection of numbers and symbols – often EMBEDDED IN A QR CODE - that is shared with the authenticator app. It establishes the initial special connection between that online service and the app.

The AISWA website displays the INITIAL SET-UP KEY as a QR CODE. (We also offer the alphanumeric version of the key in case you prefer to use it.) When you open your installed authenticator app and SCAN this displayed QR code (or type in the optional text code), the unique AISWA website key is saved to your authenticator app. The two are now connected and ready to use for TFA.

IMAGINE that this is like sharing business cards. Two entities must be able to recognise and remember each other before they can conduct business. It's a 'first introduction' to establish a new working relationship. It only needs to be done once. In this case, the website and your device have now been 'formally introduced' and they are ready to have an ongoing working relationship.

What happens from then on?

Once an authenticator app has been set up to work with a particular online service (like the AISWA website), it will generate a unique dynamic passcode for that service whenever it's required. (In reality, the codes are constantly generated and you just open the app and copy the current code when you need it.)

Each time you log in to your online service (such as the AISWA website), that one-time passcode (OTP) from the authenticator app will be used to confirm your log-in identity. A space (or boxes) to add that code will always be provided on the website.

IMAGINE *that this process is like a firm handshake that reconnects business associates who are already well known and trusted by each other. The AISWA website and your authenticator app already know each other, so you can get straight to business – i.e. retrieving the 6-digit code for the AISWA website.*

What is a 'trusted browser' and how does it help me?

A 'trusted browser' can be nominated before the TFA is verified. If the box is ticked, the TFA code will not be required for another 30 days, although your password will be. Trusted browsers are listed in your website account.

Only tick this box if you are the only person who uses your computer device. If you regularly share computers with others then you should NOT enable this. We consider that a strong secure passcode on your device (or your profile) will provide a good first level of protection. **If you don't have a password on your computer, we strongly advise that you create one.** Data security is an extremely important part of personal and professional 21C 'digital housekeeping'.

Why is my authenticator code not working?

1. Inaccurate timing: The code usually needs to be accessed and used promptly, as a new code will regenerate after a short time.

If you get an error message when adding the 6-digit code into the empty verification code box on the AISWA website, it's likely that your timing for adding the code was not quite right. The website may be looking for a new code if you were a little slow adding the first code. Just try again with the new code. It's likely to work if it was just a timing error. Don't worry, the codes will keep regenerating for as long as you need them

2. Incorrect service: Have you selected the code for the correct service? If you use your authenticator app for many different online services (which is quite common) each should be clearly named. Make sure the code you chose was for 'AISWA Website' and not another online service.

The name should be attributed automatically in the app. If it's not, go into the 'settings' associated with the dynamic code and name the service yourself. It saves confusion.

3. Incorrect process: Are you trying to set-up the account for the *first time* (a very long code) OR are you trying to just *confirm your established identity* with the 6-digit code? Think carefully about what you are trying to do and whether you are adding the right code in the right place. Try quitting the website completely and starting the process again just to be sure.