Multi-factor Sign-in Will be Compulsory

Sometimes called two-factor, sometimes multi-factor, sometimes sign-in, sometimes login, sometimes authentication…

Whatever the name, you should be using it!

A professional bookkeeper (especially external or contract), and any other advisor who has access to client data ***must*** have multi-factor authentication turned on for login and significant transactions, in our view.

This is to put you as the professional one more step towards the safety of not being the point of attack or risk for a business, and to not be the point of attack for scammers.

It is also our view that it will become compulsory very soon. The ATO are working on their "Operational Framework" – which is their renewed assessment of how technology can enable enhanced interaction between Registered Agents and the ATO and the Business. This framework is looking at all aspects of the security of technology interaction, and includes a view that multi-factor security will be required. We agree; it is now about how and when to require the separate authentication step in each process.

As the multi-factor authentication feature is made available to you, you need to adopt it.

Multi-factor Login to Relevant Applications

We have our common accounting programs (with MYOB, Inuit QBO and Xero promoting their services quite heavily) implementing this level of security at the point of access to the "file". In our view you ***must*** turn this currently optional service ***on*** for you and your respective businesses, and for all users.

In our view, you are now at legal risk if you do not turn this on when it is available. If your credentials are falsely used by another person to illegally change details which enables theft of some manner, and you did not have this multi-factor login turned on, we believe the case against you is considerably stronger. Your only out would be if the client or your employer had instructed you to leave the multi-factor requirement off, explicitly in writing. We still do not believe this to be acceptable behaviour for a professional.

MYOB and Xero have also implemented an option that your two-factor authentication on login on each device can be "enabled" for 30 days; i.e. using a particular device, you login and authenticate using a second factor, and that device is permitted to use that authentication for the next 30 days. This removes the annoying step of constantly performing two-factor every time you login, but would only remain secure ***if*** you also have good security on logging into the device.

The Risk you are Removing

The evidence is that the crooks are obtaining usernames and logins from any one of many sources. Many users utilise the same password for multiple applications. The crooks then use what is known as a "credential stuffing" technique; ie they throw many usernames and passwords at the login for a machine or application (especially cloud) to gain access. Multi-factor removes this access.

Some programs are providing a notification to you, separately to the program console, that your username has been used from an unusual location to access the program. We like this.

Some programs are providing a notification to you, separately from the program console that bank account details have been added or changed. We like this too.

Multi-factor for Significant Transactions

We also like the use of multi-factor login that some programs have implemented at the time of performing some transactions. A separate, distinct authentication should be obtained as part of the process of lodging or banking processes.

If a program is facilitating the debiting of amounts from the bank then multi-factor ***must*** be in place. A username and password is **no longer** considered sufficient security.

Typically the accounting program is creating an ABA file, and an authorised user is logging into the internet banking service and uploading the file. This internet banking should require more than just a username and password, however if the bank permits less then so be it… as long as the person logging in is actually using ***their own identity***. It is **not acceptable** for a professional bookkeeper to be logging into internet banking sites using someone else's credentials. Increasingly the bank is requiring a second form of security token provided by a dongle, device, SMS or authentication app. We believe this should be in place.

Superannuation payment systems, which seem to be effectively incorporated into our accounting programs, are already requiring an effective process of separate authentication. For example: MYOB Superannuation Payment requires a separate login and second factor via SMS to authorise the lodgement and payment.

Multi-factor Login to Your Device

In some respects, you and your data and your access could be protected if we had an effective system of multi-factor authentication at the point of logging in to your device. Because you have used multi-factor at the point of device entry, then the theory would be that you are covered for all programs on the device. We don't think this type of effective security management has been implemented. It exists on accessing some devices, but not then relaying the security to the programs you may access. This could also become very annoying, and just become another default version of a generic pin and password access.

When we have a system that can acknowledge that multi-factor was used at the point of device login, and that is relayed to each program you then access, we see that this could be effective.

Security and *Identification* Must be Enhanced

It is already law under the Tax Administration Act and the Tax Agent Services Act that only authorised persons can lodge, communicate and interact with the ATO. Before lodging an Approved Form with the ATO, a declaration **must** be obtained and stored by the person facilitating the lodgment. Not all of our software has been providing the process for you to obtain and store this declaration. This is changing, and the ATO are beginning to require it as part of any approved software.

Electronic authorisation and digital signatures are permitted.
The recently designed Single Touch Payroll requirements incorporate fields that identify who has made the required declarations. It is no longer just the “technical” AUSkey that software needs to use, but also identify the person.

The government, primarily through the Digital Transformation Agency but also led by the ATO, are developing what is called the “Trusted Digital Identify Framework”. This TDIF will provide a digital system whereby once you are authenticated into the framework, you would be able to use multi-factor including biometric systems (fingerprint, voice recognition, and now they are also talking facial recognition) to ensure it is the authorised person themselves that is performing the function.

Conclusion

- Software should provide the process for correct authentication of the authorised individual.
- Software ***must*** require multi-factor authentication.
- Software should be enabling the process to obtain the legally required declarations.
- Digital Signatures are acceptable.

Professional bookkeepers ***must*** adopt current security processes, including multi-factor authentication.

Do not use any other person's login or identity for any function at all ever.
Do not login to banking software using another person's identity.

Implementing Multifactor

- MYOB – Two-factor Authentication
- Intuit QBO – Multi-factor Authentication
- Xero – Two-step Authentication