insight

What you need to know about two-factor authentication

insight

What is Two-Factor Authentication (2FA)?

Two-factor authentication also known as multi-factor authentication simply means there are two checks in place to prove your identity.

Two-factor authentication (often shortened to 2FA) provides a way of 'double-checking' that you're really the person you're claiming to be when you log into your online accounts, such as banking, email or social media.

When you log into an online account with a username and password, you're using what's called single-factor authentication. You only need one thing to verify that you are who you say you are.

With 2FA, you need to provide two things – your password and something else such as a code sent to your mobile device or your fingerprint – before you can access your account.

This second level of authentication is not new, however, it is gaining momentum as accounts are left vulnerable with weak or poorly-secured passwords. A range of websites including Twitter, Paypal and WordPress have an optional second factor to their log-in processes, and online banking sites have used 2FA for a long time.

How do I set up 2FA?

Some online services will automatically prompt you for a second factor when you log in. However many don't, so you will need to activate it yourself. You'll find the option to switch on 2FA in the security or privacy settings of your online accounts (it may also be called 'two-step verification').

There are several types of 2FA available based on either something you know, something you have or something you are. Examples include:

SMS codes sent to your phone

Fingerprint scans

Voice recognition.

A physical device, like a security token that generates temporary access codes

Security questions set up by you, which only you would know the answers to when prompted

Software, such as Authenticator app, that sends a notification to your device or provides a temporary access code.

Do I have to use 2FA every time I access a service?

Generally, once you have set up 2FA, you should only be prompted for unusual activity such as setting up a new payee for your bank account, logging into an account from a new device, or changing your password.

Why is it important?

While it does require one extra step to a log-in process, it provides a much stronger defence for your account. If your password is hacked (accessed by someone else without your permission) and you have 2FA activated on your account—the hacker cannot gain access. They need both levels of authentication.

Having 2FA is not going to remove all risk, however, you are much harder to hack than accounts with only single-factor authentication. This means you are a much less likely target and you are reducing your risk dramatically.

If you're travelling or will not have access to your second level for a period of time, consider changing your second criteria to something you will have access to, or obtain some single-use back-up codes. Do not turn 2FA off!

We recommend:

- Wherever possible, activate two-factor authentication (2FA)
- Use strong passwords/passphrases and keep them safe
- Do not use the same passwords across multiple sites
- Use a password manager to keep stock of all your passwords and log-in details

As your IT services provider, we can take care of your 2FA set up from start to finish. We will guide you through few quick and simple steps without interruption to your day-to-day work. If you have any questions or concerns regarding 2FA set up, don't hesitate to contact us.

Email: info@my-insight.com.au phone: 1300 911 000 | 02 9299 0222