martin & white
Accountants & Business Advisors

Do you have adequate data protection in place?

We're sure many of you have been overwhelmed by the latest news of cyberattacks and data breaches. Whether you're an individual or a business it's essential to have systems in place to protect your data and yourself from fraudulent activity such as identity theft.

So, what can you do?

Passwords

DO have long passwords which have a combination of letters, numbers, and characters.

DON'T use the same generic password for all your accounts, for example "Admin1234".

RECOMMENDATION – Track your passwords using a password manager.

Set up multi-factor authentication

Multi-factor authentication requires users to provide multiple forms of identity authentication. This adds another level of security to your data e.g., input your password PLUS input a code generated and sent to your mobile.

Should a cybercriminal gain access to your password multi-factor authentication prevents a further breach of your account.

Learn more about password managers and multi-factor authentication here: https://www.cyber.gov.au/acsc/view-all-content/publications/quick-wins-your-password-manager

Be wary of phishing emails and texts

Phishing messages trick you into handing over personal and sensitive information to cyber criminals. These types of messages may be obvious at times but often they can appear genuine.

DO pay close attention to the senders' email address or their profile details.

DON'T click on any links within the message. If it seems genuine yet you're still not sure about its authenticity find an alternative way of contacting that organisation to investigate.

The Scamwatch website is a useful resource: https://www.scamwatch.gov.au/

Take a quiz here: https://www.cyber.gov.au/acsc/view-all-content/campaign/know-how-spot-phishing-scam-messages

Backup your data

Backup, backup, and backup again!

Learn more about keeping your data safe here:

https://www.cyber.gov.au/

What to do if you think your personal data has been accessed

If your personal details fall into the wrong hands, then it can be used to steal your identity.

If you think this has happened to you, report it to your bank and change your passwords ASAP. Make sure you keep a close watch for suspicious transactions. You may need to put a temporary block on your credit cards or cancel them altogether and get new ones.

There is some great information on the MoneySmart website:

https://moneysmart.gov.au/banking/identity-theft

What to do if your tax file number (TFN) has been compromised

If you suspect your TFN has been compromised, contact the Australian Taxation Office (ATO) as soon as possible. They can place extra security on your TFN while they investigate. **Ph: 1800 467 033**

The ATO will NOT:

- *ask you for your TFN or bank details via return email, SMS, or on social media*
- *give your personal information to anyone without your consent, unless the law permits them to*
- *communicate with you on behalf of another government agency or ask another government agency to represent them.*

(Source: https://www.ato.gov.au/General/Online-services/Online-security/#Howweprotectyou1)

Further information from the ATO can be found here:

https://www.ato.gov.au/general/online-services/identity-security-and-scams/help-for-identity-theft/

Published November 2022 by Martin & White Accountants & Business Advisors