CRANAGE
financial group

**CFG Cyber Security and Confidence in our Vault**

With an increased focus on Cyber Security, Cranage has been busy implementing several changes to ensure our data is secure. We have recently completed a thorough assessment of our IT systems (externally audited) and are pleased to inform you that the systems we have implemented have helped Cranage achieve the Federal Governments Essential Eight Maturity model (Australian Cyber Security Centre - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model).

In addition to tightening our systems, we are constantly reviewing and updating internal processes to further enhance data security, and we remain diligent and dependent on the industry in terms of best practise for data collection - which is minimal. For those interested, here are the details of the key security items we now have in place at CFG:

- Our staff cannot access our systems without Multifactor Authentication (MFA)
- Our PC/Laptops are encrypted, and only registered Cranage devices can access our systems
- Access to our systems is restricted to specific location – preventing international hackers
- All data is encrypted whilst in transit and at rest (within our systems)

We would like you to be confident that your personal data is safe and secure with us and want you to know that we have taken all the necessary steps to keep your information in our Vault. Please refer to our recently updated Privacy Policy for further details on how we treat your personal information.

**Steps you can take to protect your personal data at home:**

- Use Multi Factor authentication where possible
- Use unique and/or different password for all your sites and social media accounts
- Change your passwords regularly
- If you have doubts about an email, **do not click on or download anything**. A financial institution is highly unlikely to ask you to provide your credentials over email
- Do not provide any personal data via email ie TFN's, Drivers Licence, bank details, corporate keys etc
- Do not save any personal data to your desktop. Instead use a secure platform like drobox or SharePoint

**Be aware that Phishing messages or content may:**

- Impersonate a reputable organization, like your bank, a social media site you use, or your workplace
- Impersonate someone you know, like a family member, friend, or co-worker
- Look exactly like a message from an organization or person you trust