

DUAL

10 TIPS

TO HELP PREVENT A CYBER ATTACK

DUAL Australia has partnered with Cyber Incident Management Team (CIMT) to manage all cyber incidents from initial notification through to a resolution. In the first instance, if you experience a cyber claim or incident, notifications should be made via the following methods to ensure that security / privacy breaches are managed efficiently and effectively:

24/7 monitored email at cyber.incident@canopius.com or the Cyber Incident Reporting hotline on +64 483 10243.



Backup Data

Backup data frequently with the backups stored off the insured's premises and not connected to the insured's network.



Firewall & Anti-Virus Protection

Use operating systems with embedded firewalls and anti-virus protection software (such as Windows or MAC OS X), or run separate commercially licensed firewall or anti-virus protection software.



Mobile Device Encryption

Protect your data with encryption including mobile phones, laptops and other portable devices.



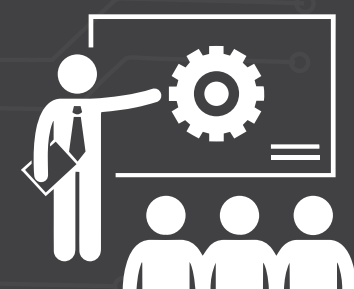
Password Protection

Keep passwords strong and secured and set up two factor authorisation (2FA).



Two Person sign-off

Ensure that at least two members of staff authorise any transfer of funds, signing of cheques and the issuance of instructions for the disbursement of assets, funds or investments.



Staff Training

Ensure all staff have frequent cybersecurity training so they are aware of the potential risks.



Never pay Ransom

Its not always wise to pay a ransom as you are not able to determine where the money will go (i.e funding terrorism without knowing) or if the hacker will repeat this attack.



Credit Card Storing

Do not store your credit card details on websites – do not keep them saved on notes or documents on your computer system.



Third Party Vendor Management

Any requests to alter supplier and customer details including bank account details, independently verified with a known contact for authenticity.



Incident Response Plan

Have a well-planned approach to addressing and managing a cyber attack to help respond to, and recover from network security incident.