




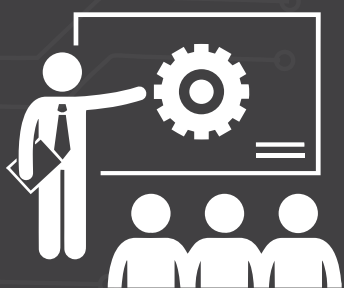








10 TIPS TO HELP PREVENT A CYBER ATTACK

DUAL Australia has partnered with Charles Taylor Adjusting 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@ctplc.com or the Cyber Incident Reporting hotline on 1300 004 880.

<p>1</p> 	<p>2</p> 	<p>3</p> 	<p>4</p> 	<p>5</p> 	<p>Backup Data</p> <p>Backup data frequently with the backups stored off the insured's premises and not connected to the insured's network.</p>	<p>Firewall & Anti-Virus Protection</p> <p>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.</p>	<p>Mobile Device Encryption</p> <p>Protect your data with encryption including mobile phones, laptops and other portable devices.</p>	<p>Password Protection</p> <p>Keep passwords strong and secured and set up two factor authorisation (2FA).</p>	<p>Two Person sign-off</p> <p>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.</p>
<p>6</p> 	<p>7</p> 	<p>8</p> 	<p>9</p> 	<p>10</p> 	<p>Staff Training</p> <p>Ensure all staff have frequent cybersecurity training so they are aware of the potential risks.</p>	<p>Never pay Ransom</p> <p>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.</p>	<p>Credit Card Storing</p> <p>Do not store your credit card details on websites – do not keep them saved on notes or documents on your computer system.</p>	<p>Third Party Vendor Management</p> <p>Any requests to alter supplier and customer details including bank account details, independently verified with a known contact for authenticity.</p>	<p>Incident Response Plan</p> <p>Have a well-planned approach to addressing and managing a cyber attack to help respond to, and recover from network security incident.</p>