AARON FISHER *CEO and Author, My Info Tech Partner*
Website www.myinfotechpartner.com.au

Aaron is the author of the book "Protect Your Legacy" and a veteran IT professional and Certified Information Systems Security Professional who has been in the IT industry since 2003. His company specialises with protecting the reputation and livelihood of the equity partners or directors of professional services firms and stopping them from making big expensive mistakes with technology. With his limited spare time, he enjoys the outdoors - be it the beach or snowboarding the Canadian Rockies

TIP 1. DON'T RECYCLE YOUR PASSWORD ACROSS MULTIPLE ACCOUNTS

This includes changing 2-3 characters, numbers or symbols in the same password. Hackers have software that allows them to try multiple combinations or variations of passwords, making it easy to break into your account if they know a version of your password. Instead, use strong, completely unique, passwords, at least 12 characters in length, ideally longer, with numbers, letters and symbols or special characters.

TIP 2. GET A PASSWORD DATABASE AND SECURE THIS WITH A PASSPHRASE

That is something only you would know; for example, a childhood memory or a favourite holiday destination. This password database, which is unlocked with your exclusive passphrase, allows you to copy and paste passwords – this way you won't have to remember all those complicated passwords you've created.

TIP 3. USE MULTI-FACTOR OR TWO-FACTOR AUTHENTICATION

Including, but not limited to, email accounts, password databases and remote access systems, such as virtual private networks. Recent changes in cyber liability insurance mean that, if you don't have this in place, you won't be able to get a quote or renew an existing policy.

TIP 4. STAY ON TOP OF INSTALLING SOFTWARE UPDATES ON ALL DEVICES

This includes your computers, mobile phones, tablets, security cameras, door access controls, home and business building automation systems - essentially anything that can be connected to the Internet, a network or Wi-Fi.

TIP 5. ENGAGE WITH A PROFESSIONAL, PRO-ACTIVE, IT AND CYBER SECURITY COMPANY

You need to review your systems, even if you're currently utilising the services of another IT services provider. Reviewing your systems before a breach will save you stress, anxiety, time loss, and monetary loss. Hackers are constantly up skilling, so this must be an ongoing service engagement, not a one-and-done.

TIP 6. HAVE A SERIES OF ROBUST, LAYERED DEFENCES LIKE THOSE YOU'D FIND IN A CASTLE

You want to have a series of advanced layered defences like those you'd find in a castle. If one layer fails, there is another and another to protect you. The layers need to address 3 key areas, those are people, process and technology. You can learn more about them with this FREE resource www.myinfotechpartner.com.au/success-kit/.

TIP 7. COMBINE ROBUST LAYERED DEFENCES AND CYBER LIABILITY INSURANCE

You can't have an either-or approach, you need to have both. There are some in the cyber liability insurance space

already exiting the market as they feel their risks are too high. You need to ensure your insurance broker and/or company is talking with your supplier to ensure what you've said you've got is being supplied. Otherwise, you may find yourself up the proverbial creek without the paddle.

TIP 8. ENSURE YOUR BACKUPS ARE WORKING AND YOU HAVE AT LEAST 3 COPIES

You want to ensure that you have working backups and that there are at least 3 copies of the data, with one completely offsite or offline from your office or IT systems. Obviously, ensure these are tested regularly to make sure they work. The worst time to find out they don't work is when you need to restore a backup ASAP and find out you can't. Then you're up the proverbial "creek" without the paddle.

TIP 9. AVOID GUEST OR FREE WI-FI WHEREVER POSSIBLE

Wherever possible, avoid connecting to any guest or free Wi-Fi networks such as those found at cafés, hotels, gyms, etc. It's very easy for a hacker to intercept your personal and confidential information including infect you with malicious software that causes a breach, with the time and monetary loss associated. If you can't avoid it, ensure you have a virtual private network that you or your IT services provider control, to connect to, before sharing any other information.

TIP 10. AVOID CHEAP OR FREE VIRTUAL PRIVATE NETWORK "SERVICES"

Just as bad as free Wi-Fi is the cheap or free virtual private network services you see advertised. One of my mentors has a saying, "If it's free, you are the product". You have no idea what they do with your browsing history or data. Naturally, they could be the cause of breach, if either they have been hacked or infiltrated by cyber criminals, or their service is operated by cyber criminals to allow easy access to their victims.

If you're the equity principal, partner, director or practice manager of a legal, accounting or financial services firm and want more FREE tips like these. Then go to www.myinfotechpartner.com.au/bec-tips/ and submit your first name and email address to receive actionable, byte sized, bad IT pun, emails to your inbox. These emails, if actioned, will help you protect your reputation, income and stop you from making big expensive mistakes with technology. Alternatively, click here www.myinfotechpartner.com.au/bec-legacy/ and sign up to receive an eBook copy of my book 'Protect Your Legacy How To Confidently Protect You And Your Firm From The FINES, LAWSUITS, CUSTOMER LOSS, RUINED REPUTATION & PR NIGHTMARE Resulting From A Data Breach And Cybercrime.