Stay one step ahead!

In Australia, a cybercrime is reported every 10 minutes. With criminals using phishing, malware, ransomware, social engineering and numerous other tactics to obtain data and other resources, it is important for organisations to keep themselves secure from cyber attacks.
To prevent the success of a cyber attack and to create the best defence against the hackers, you must first learn to think as they do.

Footprinting or searching for data

Cybercriminals will search social media for employees of your organisation and will be on the hunt for information that is shared openly. Information such as a pet's name could help cybercriminals gain access to an account by guessing a password or answers to secure questions.
You can protect yourself by making sure that your social media presence is set to private and being mindful about what you share online.

Scanning for a lack of security

Cybercriminals will scan an organisations online presence and look for a way into their system, just like looking for an open or unlocked door into a building.
You can protect yourself by making sure that your cyber security hygiene is being upheld by:

- having firewalls and antivirus in place
- using strong and unique passphrases with a password manager
- making sure that there is no out-of-date software and that all security updates and patches are maintained
- making sure staff download information with care.

Preying on a lack of awareness

Cybercriminals will use social engineering tactics including phishing to trick employees into divulging their personal information or log in credentials through fake or malicious emails.
You can protect yourself by knowing the signs of a social engineering attacks such as phishing emails and smishing through cyber awareness training and knowing what to do when receiving a potential email scam.

Making a system vulnerable

Cybercriminals will try and install unapproved or untrusted applications such as malware and ransomware in an organisations system to cause an internal attack.
You can protect yourself by:

- keeping your system and applications up to date with necessary updates
- perform regular backups of your digital information
- implement access controls to limit who can access specific information
- always use anti-virus software.