Cyber Security Tips

1 Software and Virus Protection

- Remove unsupported or outdated applications from the network
- Apply all security updates to operating systems and browsers
- Perform regular, tested backups to ensure data recovery
- Use optimal business security software with up-to-date antivirus protection

2 Payment Processes

- Never trust bank account details sent by email
- Advise clients and payers to follow the same caution
- Always verify details in person or via a known phone number
- Make outbound calls only to trusted contacts
- Confirm the identity of the person and double-check account info
- Use Multi-Factor Authentication (MFA) whenever possible

3 Data Security

- Ensure staff understand obligations under the Privacy Act 1988
- Implement strong information management and protection procedures
- Restrict access to sensitive data based on least-privilege principles
- Secure and regularly verify backup processes
- Require Multi-Factor Authentication (MFA) wherever possible

4 Plan Ahead

- Have a Cyber Incident Response Plan in place in case your systems are compromised or disabled, and regularly test the plan by running tabletop exercises

5 Staff Awareness & Preparedness

- Establish clear policies and provide training on cybersecurity
- Use unique passwords and update them regularly
- Raise awareness of risks, for example:
  - Clicking suspicious links or attachments
  - Using unsecured or public WiFi
  - Importing files via USB/external drives
- Implement proper security checks for workplace visitors, especially those accessing IT systems

6 Seek Advice

- Cyber risk management is essential in legal practice
- Seek expert help from IT consultants and risk advisers to assess your needs
- Act immediately on suspected breaches—contact the cyber incident response team at **1800 4BREACH (1800 427 322)**