Lawcover

Email Cyber Fraud
Be Aware and Prepared

1. VIGILANCE

- Adopt a less trusting and more critical mindset as requests by email regarding money transfers may be fraudulent
- Develop secure anti-cyber fraud policies for managing emails, especially requests for money transfers or for change of bank account details

2. INFORM

- Your staff of the policies and ensure they understand and follow them
- Your clients that you will never change your account details by email and that they should inform your office in the event they receive an email indicating otherwise

3. VERIFY

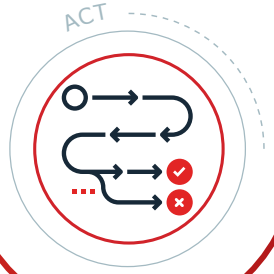
- When an email contains instructions to transfer funds into a specific account, verify the identity of the sender, be it a client, another lawyer or perhaps a real estate agent
  - call the sender of the email by telephone, using a credible number such as from the original instructions (ie: NOT contained in the suspect email)
  - confirm the email is from the expected individual and request confirmation of the valid account number and perhaps one other valid piece of information to confirm their identity

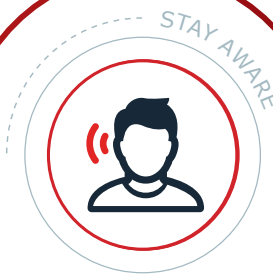
4. RECORD

- Make a file note of the time of your call and the details provided to you

5. ACT

- If the verification is correct, continue with normal processes
- If the verification fails, contact the incident response team at 1800 BREACH (1800 273 224) and inform them you suspect you may have been subject to a cyber event
- Follow any instructions given to you which may include informing the owner of the email account about the incident if it appears they have been hacked





6. STAY AWARE

- If you or one of your colleagues are subject to a cyber event or fraudulent activity, share the information within your office, learn from the steps taken and remind everyone of your anti-cyber fraud policies