

# Client Cyber Alert

## Funds transfer critical information

Clients of law practices across Australia **have lost money** when hackers have impersonated the practice in emails. If you want to protect your money the following steps are critical:

### DO NOT

Transfer any money (cheque deposit or electronic transfer) more than \$10,000 **without first** telephoning to verbally confirm the account number, details and amounts by **reading out and reading back the account and BSB numbers**.

### DO

Contact, by telephone, to confirm verbally the bank account details for any payments I expect to receive by **reading out and reading back the account and BSB numbers**.

### DO

Give the same warnings to anyone else we know who is involved in the matter (e.g. the agent, broker, family member involved or any other party) that may also be involved in transferring money.

Also:

- ensure that you do not contact us using a phone number listed in any communication from you that asks for money or sets out account numbers or details **without first** checking the phone number in a prior separate paper communication from us or checking our website or white or yellow pages telephone listing.
- contact the sender to check legitimacy **before** you open attachments, click on hyperlinks or download buttons in unexpected emails.
- contact our law practice if in any doubt about emails or other electronic communications that appear to have come from us.

**PLEASE NOTE:** we will not transfer money out of our practice until we are able to verify any bank account by a voice call to confirm those details (**by reading out and reading back the account and BSB numbers**). **You must make sure you can be contacted if you need any funds transferred by a specific time.**