ambrylegal
TAXATION & BUSINESS LAW

Law firms and their clients are targets for cyber fraud including email compromise, payment redirection fraud and ransomware attack. Here are some precautionary measures we can all take to ensure the security of your information and money transfers.

What we will do

- Tell you at the start of a matter what our payment details are and not change those details unless we speak to you first. We will never notify you of a change in bank account details only by email.
- Always authenticate and verify email instructions from you that direct where money should be sent by speaking to you in person or by phone.

What you must do

- Before transferring money always call or visit the person handling your file or another known contact at the firm to verify you have our correct account details.
- Never respond to an email that purports to be from us requesting you to pay money to a bank account that is different from the account that we gave you at the start of the matter.
- Contact our office by telephone or in person if you receive any unexpected or suspicious email purporting to be from us.
- Follow some basic cyber-crime prevention steps including:
    - keep all software on your devices up to date with all updates and security patches installed
    - have different passwords for everything. Make sure they are at least eight characters long, and contain capital letters and numbers, and change them at least every 12 months
    - keep an eye out for phony or fraudulent emails. Don't respond to emails that ask for personal information as legitimate companies will not use email to ask for your personal information
    - don't open attachments or click on links embedded in emails from people you don't know.
    - implement multi-factor authentication for all devices
    - check your email rules regularly to make sure any rules that are there have been created by you and not a cyber-criminal who has gained access to your emails