Cyber Security

how to protect yourself

Law firms and their clients are targets for cyber-criminals and cyber fraud. Cyber-criminals are experts at intercepting and modifying emails containing sensitive information including bank account details to try and divert your money to their bank account.

Often, there is no indication that an email has been compromised, as it will appear to be from a legitimate email address. Once funds are diverted, there is generally no or limited recovery through the banks.

Here are some precautionary steps you must take to protect yourself against cyber-crime and potential loss. We will also take steps to prevent the loss of funds.

WHAT YOU MUST DO

- Never rely on or trust emails from our law firm providing bank account details. Treat all emails and electronic documents, including PDF documents with suspicion, as if they may have come from a cyber-criminal or not legitimately sent by us.
- If you receive an email containing bank account details and requesting payment, you must call or physically see a known contact at the firm to verify the authenticity of the email and ask them to verbally confirm the correct bank account details.
- When calling us to verbally verify bank account details, do not use contact details from an email, even if it looks like the email came from our office. Always use a known telephone number or independently search our website.
- Never transfer money without first verbally verifying bank account details with us by phone or in person.

WHAT WE WILL DO

- We will tell you at the start of our work together what our payment details are and not change those details unless we speak to you verbally first. We will not notify you of a change to bank account details by email only.
- We will call you to verify bank account details you send to us by email on a known telephone number that we will ask you to provide at the start of our work together.