CYBER FRAUDSTERS WILL GET IN ANY WAY THEY CAN. MAKE SURE IT'S NOT THROUGH YOU.

1. IDENTIFY

Don't accept email requests on face value. The email asking you to re-direct money might look genuine, but it could have been sent by a hacker.

2. VERIFY

Call the sender personally to check authenticity. Use a number you know, not one suggested in the email. Ask for the account number, write it down, then compare with the email.

3. NOTE

Make a file note that you made the call and confirmed the payment instructions, so you can prove it.

4. WARN

Tell the client they might also be targeted with fake emails from you and not to act on email payment directions without calling to check. Put this in your engagement letters.

5. DOUBLE-CHECK

Involve a second person in the process and don't action payment requests without proof that steps 2 and 3 have happened.

DON'T FALL FOR IT!

Cyber thieves are clever. They target lawyers because we direct transfers of money and they want to steal it.

BE SUSPICIOUS OF EMAIL INSTRUCTIONS.

IF YOU SUSPECT FUNDS HAVE BEEN STOLEN, STOP PAYMENT AT THE BANK IMMEDIATELY.

FIND OUT MORE ABOUT CYBER SECURITY AT LPLC.COM.AU

THE LAW SOCIETY OF TASMANIA

P (03) 6234 4133 | E info@lst.org.au