

Cyber Security – Important Information

Please read carefully - Fraudsters are actively targeting solicitors' clients

In recent months clients of various firms of solicitors have been tricked by criminals into handing over significant sums of money.

The most common type of fraud is where the criminal 'clones' a firm of solicitors and sends you an Email which looks like it comes from your solicitor.

Often payment of fees or other monies, such as deposit monies for a house purchase, is requested and bank account details are provided. You are asked to make a direct transfer into the bank account details provided. The Emails can look very convincing, and in some cases it looks as though the Email has come from the firm because the sender's Email address is the same as (or very similar to) the correct Email address.

Another common type of scam is where your Email address is cloned or hijacked and an Email is sent to your solicitor pretending to be from you and asking for monies to be paid from your solicitor to the fraudster's bank account. Because of this we will never accept instructions to send money to you by Email alone, but will always verify these instructions with you by telephone or face-to-face. Until we have verified your identity and bank details to our complete satisfaction we will not release any monies to you. It is therefore important that you return our telephone calls or respond to our letters promptly. If you do not, then there may be delays in you receiving any monies which we hold on your behalf.

The clients of this firm have never been targeted in these kinds of scam, but it is important that you are alert to the possibility that you could be targeted. We run strict information security, data protection and client confidentiality programmes, but it is important that you remain vigilant too. There is further information in our terms of business, in the section headed 'Confidentiality, Privacy and Data Protection'.

Please note that we will never ask you to make a payment directly to our bank account by Email. Any such Email you may receive will not have come from this firm and should be reported to the police and to us immediately.

It is your responsibility to conduct your own due diligence by checking the authenticity of any Email from us by contacting us directly by reliable and established means, such as by telephoning the number on our website (not the number on any suspicious Email you may receive). Email is not a secure form of correspondence. You can ask us not to correspond with you by Email at all if you wish, or we can set up a secure and encrypted Email system with you upon request.

If you do not follow the advice above you could stand to lose significant sums of money to fraudsters and this firm will not be liable to you for any losses unless they have occurred as a result of our negligence.

Further information about fraud and cybercrime can be found on the Solicitors Regulation Authority website at <http://www.sra.org.uk/consumers/problems/fraud-dishonesty/scams.page> or on the Action Fraud website run by the National Fraud Intelligence Bureau at <http://www.actionfraud.police.uk/>

If you have any other concerns or questions, please discuss these with us straight away,