STAY SAFE

PROTECT YOURSELF FROM CONVEYANCING FRAUD

Conveyancing fraud occurs when criminals pose as your solicitor, usually by intercepting email communications to trick you into sending money to their bank account.

How the fraud works

Email Hacking

Criminals hack into email accounts to monitor the conveyancing process. Your personal email account is their preferred entry route.

Impersonation

Fake emails with modified bank account details, with the criminal posing as Taylor Walton.

Deposit Diversion

You are then tricked into transferring your property deposit or balance to complete to the fraudsters' bank account instead of the genuine one.

TAYLOR WALTON'S TOP TIPS TO STAY SAFE:

Verify payment details

Bank details are sent by post to your home at the outset – please retain these.

We allocate you 3 words at random at the outset of your case and these words are sent to you within the bank details letter. Please retain these as we may ask you to provide these words to securely identify you during the transaction.

Please do not provide your bank details to us by email. Please provide via post. We will always verify these with you via telephone before we send funds to you.

Only send funds we have requested from you.

Call us to verify the bank details you have – use our main switchboard numbers to make this call and speak to someone in our residential property department.

Timing of funds requested in transaction

We request funds:

- at the outset on account of costs (£500 per matter only);
- during the transaction for items such as management packs or planning documents;
- for purchases; deposits immediately prior to exchange and balances to complete a week or so before completion.

BE ALIVE TO SCAMMER TACTICS!

Look for poor grammar, spelling mistakes and/ or unusual wording. Check the email address is correct. Fraudsters will often change just 1 letter, e.g. a “1” instead of an “l”.

Bank Details will not be sent by us to you by email so if the email contains bank details it’s not from us!

Do not transfer funds or send any personal information if you feel pressured to act quickly or if something does not feel right.

Protect your devices and account

Strengthen your email and device security by using strong passwords, multi-factor authentication and anti-virus software. Avoid using public Wi-Fi for sensitive transactions.

Do not use unprotected public Wi-Fi for accessing sensitive information or performing banking transactions, as fraudsters can hack these networks.

Avoid posting on social media about your property purchase, as this can alert criminals to your situation.