

Avoiding Cybercrime in Conveyancing

Top Tips to prevent conveyancing fraud and avoid losing your money

QUICK TIPS

Section 1. Some General Tips on Detecting Cybercrime:

- Don't send money to your conveyancers account if it is different from the details found on your secure client portal.
- Don't send money to any conveyancer account which is set out in an email.
- Don't trust conveyancers emails that don't come from their own specific domain emails. For example ours ends in @avrillo.co.uk. Emails from Gmail accounts from conveyancers risk being fraudulent.
- Don't trust emails containing spelling or grammar mistakes, or addressed to 'Dear Client'.
- Don't trust 'call back' numbers - use numbers you trust.
- Don't click on 'contact us' or 'email us' links in emails, type in an email address you know, type in web addresses you know, and call your individual conveyancer.
- Don't give anyone your confidential information (bank account details, passwords, user IDs, payment card details on websites unless from a secure address starting with https:// not http ('s' stands for secure). Don't give clues to such confidential information on social media (e.g. Facebook).

Further advice

See 'The National Cyber Security Centre' <https://www.ncsc.gov.uk/>



Cybercrime & Conveyancing

Conveyancing is an extremely high risk area for cybercrime. It is being increasingly targeted by criminals who defraud buyers and sellers out of millions of pounds simply by asking them to transfer money to false accounts on the strength of no more than an email or phone call containing bank details and the sum to be transferred. They are using a combination of fraudulent methods including intercepting emails, setting up false email accounts purporting to be from your actual bank. Unfortunately, all buyers and sellers must now be alert of being hacked as the fraud can include you being sent an incorrect bank account for you to make payment to. Similarly your conveyancers can be sent an incorrect bank account from someone impersonating you, asking your conveyancer to forward your money to that incorrect and fraudulent bank account.

Fake Emails

Emails are not a secure method of communication. This means there is a significant risk of cybercrime fraud happening in conveyancing. Criminals will use methods such as hacking into your computer and sending fake emails pretending to be from your conveyancer. The email may look very convincing and as if it is from your actual conveyancer. This is because the fraudster may have infiltrated your computer and read your emails.

Once they have hacked your email, it makes it very easy for them to find out if you are buying or selling, copy your property address, case reference as well as other details which they will use to commit a fraud on you by cybercrime. They can also replicate your conveyancer's logo and branding so look very carefully at emails. The fraudster's ultimate goal will be to convince you to send your money to their fraudulent bank account (and you will likely lose your money forever to that criminal). In law, it is your responsibility to be alert to this potential cybercrime as you will be responsible for your own loss if you send money to the criminal's incorrect account. It is likely to be lost forever.

Here are three example warning signs of fraud you should lookout for:

1. An email asking you to send money to a bank account. This is indicative of a fraud as conveyancers should not be asking for money by email, nor should they set out their bank details in an email.
2. A difference between the bank account set out in their email and the one your conveyancer would have sent you by post, in their initial letter. If the account is different you are likely to be the target of cyberfraud.
3. A change in your conveyancer's bank account details. Conveyancers do not normally change their bank account, and if they do, will never notify you by email or set out new bank account details by email. So look out for a conveyancer changing their bank details.

QUICK TIPS



Section 2. Tips protecting yourself against Cyberfraud Hacking:

- Use a 'firewall' on your computer to prevent unauthorised access.
- Install anti-virus software on all devices, i.e. computers, tablets, and mobiles you send and receive emails from.
- Keep all of your software and operating systems up to date.
- Don't allow anyone physical access to your computer, including remote access over the internet.
- Do not install any software on your computer unless it is from a trusted source.
- Create secure passwords which are long, mixing random numbers, lower and upper case letters and are unique to you. Change your passwords regularly.
- Do not use public Wi-Fi to send or receive emails or to enter your bank account details online.
- Don't open suspicious or unknown emails.
- Don't click on attachments in suspicious emails, texts or pop-up messages.

Immediate Steps

Suspicious? Call your conveyancer.

Actual Fraud? You must report to:
Firstly, 'Action Fraud' on **0300 123 2040**
or at **www.actionfraud.police.uk**
Secondly, to your own Bank.



Fake Phone calls

Fraudsters also telephone buyers and sellers pretending they are from their conveyancers or their bank or even the police, when they are not. Do not assume any call is genuine, even if your telephone display shows the correct number of the person they are impersonating. This can be replicated as it is relatively easy for criminals to find out basic information about you.

The fraudster will be looking for you to part with your confidential information such as bank details so that you can part with your money.

Below are six warning signs of fake calls

1. If the call is unexpected.
2. If the caller asks for your bank or personal details, such as your 4- digit card PIN or your online banking password.
3. They ask you to transfer money to a new account for fraud reasons, even if they say it is in your name.
4. Is there as sense of urgency from the caller?
5. Are they asking you to do something quickly?
6. Has the caller made an unusual request?

Fake Texts

Also watch out for text messages scams that:

1. Request you for sensitive, personal and financial information.
2. Have an urgent tone to their message.
3. Ask you to call back a telephone number other than your conveyancer's actual original telephone number they supplied you (for AVRillo this is 0208 370 3877).

What to do if you are suspicious?

Contact your conveyancer (on the telephone number they sent you by letter at commencement of your case) and report your suspicion to them.

How to call your conveyancer, bank or police?

Call them on a different phone from the one they called you on. This is because fraudsters have a trick of making it appear their call was disconnected, but when you make your return outgoing call to what you think is your actual conveyancer, you will be speaking to a fraudster as they have not actually been disconnected.