Avoiding Cybercrime - Client Guide

How might it affect me? | Top Tips to prevent fraud | Email and phishing

Top tips on PC safety

- Install **anti-virus software** on all your Windows or Android computers, phones, or tablets
- Do not use **public wi-fi** either to send or receive emails or to enter your bank account details online
- Do not install any software on your computer unless it is from a **trusted source**
- **Use a 'firewall'** on your computer to prevent unauthorised access
- Do not let anyone that you do not trust get physical access to your computer
- Do not allow **anyone** to get access to your computer over the internet for any reason at all
- Keep all the software and operating systems on your computers and tablets **up to date**
- **Don't open suspicious** or unknown emails or attachments
- **Don't click on attachments** in suspicious emails, texts, or pop-up messages
- **Do not give anyone your bank account details** or your passwords, or user IDs, or your payment card details on websites, unless the site is secure and the web address starts with https:// not http (the 's' stands for secure)
- Create **secure passwords** which are long, **unique for each website,** and use a mix of random numbers, and both lower and upper case letters.
- Make sure you change passwords regularly, and don't share them
- Or use a **password manager app** to create secure passwords and save you having to remember or insert them. iPhones and Macs have a secure Passwords app built in - use it.
- **Check your bank statements regularly** for unauthorised activity and notify your bank immediately, should you find anything unusual
- **Don't put important information on Facebook**, or other social media, that could give clues about your passwords used, such as birthdays, addresses, family names, or bank information, etc.

Cybercrime & conveyancing

Conveyancing clients and conveyancers have been targeted increasingly by sophisticated fraudsters over the last few years. Fraudsters have realised that often millions of pounds are sent around the UK banking system on the strength of no more than an email or phone call containing bank details and the amounts to be transferred.

They have developed sophisticated ways of diverting this money by a combination of identity theft, intercepting emails, and persuading firms and their clients to transfer large sums of money to the fraudsters' accounts by impersonating solicitors, banks and property owners.

Usually none of the money is ever recovered, and the conveyancers and clients lose out. The banks even call this 'Friday Afternoon Fraud', in fact. As a result, banks will sometimes delay completion money transfers that they suspect could be fraudulent so they can be investigated. This can cause havoc with conveyancing chains on a Friday afternoon.

Where a fraudster tricks a buyer or seller or their conveyancers to send money to the wrong bank account, the innocent clients may lose the money completely. If a fraudster impersonates the true owner of a property, and then sells the property to an innocent buyer (usually by fooling the conveyancer acting for the fraudster too), the buyer will lose all their money and there is unlikely to be any insurance to cover the loss or any way of getting the money back. Usually there will be years of expensive litigation as a result, too.

You cannot assume that your conveyancing firm will make up the loss from their insurance - it is your responsibility to be alert to fraud attempts too.

Sometimes the fraudsters will hack into your computer, and then send fake emails pretending to be your conveyancer or bank, or they perform sophisticated telephone frauds, impersonating your bank or your conveyancer.

Last year, approaching 2 million people were the subject of identity theft, and it has been estimated that the amounts involved exceeded £2 billion.

ActionFraud

National Fraud & Cyber Crime Reporting Centre

0300 123 2040

www.actionfraud.police.uk

Elderly people

Elderly people may not realise that emails and phone calls are scams, so they are ruthlessly targeted by fraudsters. If you fear that your parents or relatives may be subject to scams, ask your conveyancer to put a restriction on their title or use the Land Registry property alerts service.

Hospital or long-term care

Vulnerable people or those who are not living at their property are also targets. Again, make sure the address registered for service of documents at the Land Registry is not the property. Tenants carers, lodgers or neighbours have been known to create elaborate scams. Your conveyancer can advise on steps you can take to protect against fraud in such cases.

Buy-to-let landlords

Often tenants pretend to be the landlord, and then remortgage, or even sell the property.

In one case, a tenant stole the landlord's identity and re-mortgaged the property no less than 17 times on the same day, disappearing overseas with the money - leaving the landlord to try to persuade the various banks that there had been a fraud.

Mortgage-free houses

If you have repaid your mortgage, consider entering a restriction on the register or subscribe to the Land Registry Property Alert service.

Empty properties

As well as identity theft, some audacious fraudsters will break into properties that are empty, remove the contents, perhaps refurbish them, and then rent them out to tenants. One such fraudster in London had a successful business doing just that with at least a dozen properties.

Where the fraudsters trick a conveyancer into sending money to the wrong bank account, or to a fake firm, then sometimes the conveyancing firm will make up the loss or claim on their professional insurance if it is their fault.

Even where the fraud is spotted in time, the delay will often cause one party or the other in a property transaction to be in breach of contract for days or weeks, resulting in breach of contract claims and litigation.

However, if the fraudster has broken into your computer or impersonated you, usually then instructing your conveyancer to send money to the fraudster's account, then generally you will have to bear the loss, and the conveyancing firm will not be liable to compensate you at all. This is why you must keep your computer and email accounts secure at all times. You need to be vigilant at all times to anything unusual in the transactions or email correspondence.

Bogus conveyancing firms

There have also been an explosion of bogus conveyancing firms. Some have been so convincing that they have even fooled the solicitor's own regulatory body into registering them on the regulator's official register of solicitors.

Fraudsters often set up websites and email accounts that are virtually identical to those of a real conveyancing firm. They have even set up actual conveyancing offices, complete with staff, as spoof conveyancing outfits. One such fraud took 2 years to set up, cost the fraudsters £60K to put together - but on one single day they defrauded £6.8M before disappearing with the money.

So only deal with a reputable conveyancer that you know and trust. Only deal with the person you know at that firm, and be suspicious if you get emails or calls from someone you have never heard of, perhaps asking to you do something out of the ordinary conveyancing process.

Phone scams - 'Phishing'

Fraudsters may phone you claiming to be your conveyancer, agent, financial adviser, surveyor, bank or other lender (or even claiming to be the police or HMRC) perhaps saying your usual contact is on holiday, and ask for personal information, bank details or passwords.

If this happens, stop and think. Is the information being asked for reasonable sensible? Is it something that you would expect the caller to have already, is there an unexplained sense of urgency? Are they asking for bank details or passwords, for example that they would normally already have?

These are all red warning signs, and great care is needed. Do not just assume that a call number (or email address) is genuine, despite how it appears on your phone or PC. Fraudsters often clone the telephone number and appearance of the emails of the firm that they want to impersonate.

Email scams

As with phone scams, the emails may be very convincing - but this could be because fraudsters have infiltrated your computer, and have been reading your emails to find out what you have been doing. The emails may seem to come from your conveyancer, and may have the same logos and references - but they will be fake. The email address shown at the top of the email may not be the real email address it has been sent from. Also it may be ever so slightly different, such as have a dash or full stop inserted, or come from a .com address rather than the .co.uk address of the firm.

Warning signs include:

- Sudden urgency for no apparent reason, such as a buyer or seller who is setting short deadlines for completion or using overseas trips or holidays as an excuse for the urgency
- Last minute changes to your bank or lending arrangements, or the lending arrangements or the conveyancer used by your buyer or seller
- Last minute requests for more money from your bank or conveyancer for no genuine explicable reason
- Sellers that don't seem to know much about the property, can't reply to reasonably pre-contract queries from you or your conveyancers, or and just want to sell it quick with no questions
- Sellers who cannot produce the usual documentation or receipts for anything
- Requests to pay the seller any money or deposit direct, or cash discounts
- The price changing suddenly, or being asked to pay a different price on completion from the price stated than on the contract or transfer
- Valuations that don't fit with the price you are paying for the property
- Emails or letters containing spelling or grammar mistakes, or addressed to 'Dear Client' or using phrases that aren't common in this country, or in normal business correspondence
- Don't trust 'call back' numbers or 'direct lines' with different area codes, or mobile numbers - only call land-line main switchboard numbers that you know to be correct, and can trust
- Don't click on 'contact us' or 'email us' links in emails - type in an email address that you know to be correct, or type in the web addresses you know, or call the person you know at your conveyancer
- If the deal or the price seems too good to be true - it usually is! Sometimes people impersonating a seller will offer a property at a cheap price on the basis it goes through quickly with no queries.
- Finally, check all amounts and bank information given to you by your conveyancers, and cross check that there have been no changes.

Ultimately, the fraudsters, masquerading as your conveyancers, will ask you to send money to a new bank account, with an excuse such as the firm's bank has just changed. Note that, in reality, firms rarely ever change their bank accounts.

Bank Scams

Fraudsters are increasingly targeting consumers over the telephone, posing as bank staff, police officers, and other officials, or companies in a position of trust.

Often the fraudster will claim there has been fraud on your account and that you need to take action. Note that your bank or the police will never:

- Phone you to ask for your 4-digit card PIN or your online banking password, even by tapping them into the telephone keypad.
- Ask you to withdraw money to hand over to them for safe-keeping.
- Ask you to transfer money to a new account for fraud reasons, even if they say it is in your name.
- Send someone to your home to collect your cash, PIN, payment card or cheque book if you are a victim of fraud.

Your bank will also never ask you to check the number showing on your telephone display matches their registered telephone number. The display cannot be trusted, as the number showing can be altered by the caller.

What to do if you have any suspicions

if any of the events mentioned in this guides happens, take great care. If its a phone call, hang up, wait five minutes to clear the line, or where possible use a different phone line, then call your bank or card issuer on their advertised number to report the fraud. Be aware that fraudsters can stay on the line and make it appear that the call has been disconnected, but when you make an outgoing call thinking you're calling the firm or organisation, the fraudster may still be on the line and have someone pretend to be the switchboard and then 'put you through' to them again. Always call the main switchboard number that you know to be the correct one, never a 'direct line' they may have given you.

If you don't have another telephone to use, call someone you know and trust to first to test and make sure that the telephone line is free.

If you are unsure about any email, contact your conveyancer, and speak in person to a someone you know there and have spoken to already.

If in any doubt:

- Call your conveyancer

- Report any fraud to Action Fraud on 0300 123 2040 or www.actionfraud.police.uk

- Call the Land Registry fraud hotline on 0300 006 7030 (Monday to Friday, 8.30am to 5pm)

Further Advice:

See the GOV.UK page on protecting your property from fraud:

www.gov.uk/protect-land-property-from-fraud