



The UK's costliest scam? Lloyds Bank warns of worrying rise in conveyancing fraud

- **Reported conveyancing scams increased by 29% last year**
- **Hacked emails allowing fraudsters to intercept property deposit payments**
- **Victims losing £47,000 on average, but for some it's more than £250,000**
- **Around 45% of victims aged 39 or under, with first-time buyers at particular risk**

Homebuyers are being targeted by criminals hacking emails to exploit the conveyancing process, with increasing numbers tricked into sending their property deposit to fraudsters.

Analysis by Lloyds Bank of conveyancing scam reports made by its own customers found they rose by more than a quarter (29%¹) in the second half of last year.

While the overall number of cases is much lower than for other types of fraud, the average amount stolen was the highest, at around £47,000 per victim. The bank has also seen several cases where victims have lost more than £250,000.

| Example scam types | Average loss |
|-----------------------------------|----------------|
| Purchase | £498 |
| Romance | £6,340 |
| Investment | £9,037 |
| Conveyancing⁽²⁾ | £47,527 |

With around 45% of victims aged 39 or under, first-time buyers may be at particular risk from this type of scam, given they have no previous experience of the homebuying process.

How a conveyancing scam happens

- Conveyancing scams typically start when either the solicitor or homebuyer has their email account hacked.
- Fraudsters will monitor email exchanges related to the property purchase, waiting for the opportune moment to strike and send false payment details.
- Sometimes the fraudster can send emails directly from the solicitor's email account, but usually they will create a spoof email address which looks very similar.
- Because they have seen the genuine chain, the emails they send will look extremely convincing, using the same names, logos and signatures.
- In some cases, the fraudsters may call the victim and impersonate someone working at the solicitors, to reinforce the urgency of making the payment.
- The homebuyer is then tricked into sending their money to a bank account controlled by the criminals.

Liz Ziegler, Fraud Prevention Director, Lloyds Bank, said:

“Buying a new home is one of the most exciting moments many of us will ever experience. But it can also be incredibly stressful, given the amount of money involved, and the need to navigate a complex legal process.

“While the financial consequences of these scams are severe, the emotional toll can be even greater. The fraud often leads to the collapse of a property transaction, with a devastating longterm impact on those involved.

“Fraudsters prey on weaknesses in email security and exploit a conveyancing process that most people may only experience a handful of times in their lives. It’s vital that solicitors also grasp the importance of educating their clients on the risk of this type of scam and make a point of sharing payment details in person at the start of the homebuying process.”

How to protect yourself from conveyancing scams

- **Verify payment instructions** – confirm payment instructions with your solicitor in person, or over the phone using a phone number you trust, not from an email or invoice. You should do this at the start of the homebuying process.
- **Be wary of changes** – solicitors very rarely change their bank account details. Be extremely wary of any sudden changes and remember that email is not a secure communication channel for receiving payment instructions.
- **Secure your email** – use strong, unique passwords and enable two-factor authentication on all your email accounts. Always sign out of accounts if using shared devices and avoid using public or unprotected Wi-Fi connections.
- **Avoid bragging online** – don’t shout about your property purchase on social media, at least until you’ve got the keys in your hand. Criminals monitor posts and will target the email accounts of those who look to be in the process of buying a new home.
- **Don’t be pressurised** – fraudsters will try to put pressure on you to make a payment at short notice or risk the deal falling through. Never send money until you have picked up the phone and spoken to your solicitor on a trusted number.
- **Pay attention to warnings** – your bank might provide a warning about the payment, especially if the name of the account you’ve entered doesn’t exactly match the details of the receiving account. Always follow the advice provided as part of any warning.

Chloe’s story

Chloe*, a first-time homebuyer in Birmingham, was thrilled about purchasing a two-bed flat for £195,000. Throughout the process, she communicated with her solicitors primarily via email.

As the completion date approached, Chloe’s solicitor promised to send her the bank details for transferring the deposit. A few days later, she received an email that seemed to be from her solicitor, complete with an invoice and payment instructions.

However, this turned out to be a cleverly crafted spoof email from a fake account.

The email instructed Chloe she'd need to make the payment to an accountant, rather than directly to the solicitors. It also advised her to transfer the money in instalments.

But first, she was asked to transfer £10 as a 'test payment'. Another email, again seemingly from her solicitor, confirmed receipt.

Next, Chloe attempted to pay the first instalment of £5,000 via her mobile banking app. Before she could complete the payment, her bank provided a warning through the app which advised her to verify the payment details by calling her solicitor directly. Ignoring the warning, Chloe proceeded, assuming the details were accurate because she had made the test payment.

Once again, she received an email from her 'solicitor' confirming the payment had been received and urging her to proceed with the next instalment.

However, when she tried to transfer another £5,000 a short time later, her bank immediately blocked the transaction due to the frequency of high-value payments, which it thought was unusual. The bank's fraud team spoke to Chloe and advised her to contact the solicitor on a trusted number.

To her dismay, the solicitor confirmed they had not yet sent her any payment details, nor received any of the money she had transferred.

She had fallen victim to a scam. Now faced with the stress of potentially losing her property, Chloe needed to raise an additional £5,000 to replace the money lost from her deposit.

The source of the email hack - whether Chloe or her solicitor - remains unclear.

**name changed to protect the victim's identity*

Methodology

Figures based on analysis of relevant scams reported by Lloyds Banking Group customers, including customers of Lloyds Bank, Halifax and Bank of Scotland between January 2023 and April 2024.

- 1) 29% increase based on the number of cases reported in the period July-December 2023 compared with January-June 2023
- 2) Conveyancing scams are categorised as a subset of 'invoice and mandate' scams, in line with UK Finance reporting standards.

Media contacts:

Lynsey Cheshire Willis: lynsey.cheshire-willis@lloydsbanking.com / 07595 124 29

Gregor Low: gregor.low@lloydsbanking.com / 07500 078 879

"This report is prepared from information that we believe is collated with care; however, it is only intended to highlight issues and it is not intended to be comprehensive. We reserve the right to vary our methodology and to edit or discontinue/withdraw this, or any other report. Any use of this information for an individual's own or third-party purposes is done entirely at the risk of the person making such use and solely the responsibility of the person or persons making such reliance."

© Lloyds Bank plc all rights reserved 2024.