Keep Your Money Safe

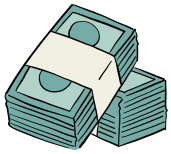
Surrey Police and Sussex Police Fraud Newsletter

In this issue

"Each month we see many incidents of fraudsters targeting our residents in an attempt to defraud them. We're working hard to prevent this and support vulnerable victims of fraud or scams. By following our tips and encouraging family, friends and colleagues to do so too, you can reduce the risk of becoming a victim."

Detective Chief Inspector Simon Doyle, Surrey Police & Sussex Police Economic Crime Unit

What is rental fraud?



Rental fraud happens when would-be tenants are tricked into paying an upfront fee to rent a property. In reality, the property does not exist, has already been rented out, or has been rented to multiple victims at the same time.

The victim loses the upfront fee they have paid and is not able to rent the property they thought they had secured with the payment.

The impact this can have on victims goes beyond the financial loss, with some having terminated their previous tenancy agreements and cancelled contracts before realising the fraud. With the effects of the recent rise in the cost of living, individuals look to seek cheaper rent for properties and so become more vulnerable to being taken advantage of.

Typically victims lose between £500 and £1500, having sent what they believe to be the deposit to secure the contract on the property. Often the properties are being advertised on multiple websites and social media platforms at the same time.

Case Study

In one recent Sussex example a victim contacted the landlady on a website called House Ladder. He was pressured into paying a sum of money to secure a viewing of the property which he transferred to the account provided. On receipt of the money a contract was sent and he was asked to send a further sum of £500 which he promptly did. On being asked for more money he became suspicious and tried to arrange a viewing, but found he was unable to make contact and had been blocked by the landlady on Whatsapp.

How to spot a rental scam:

- Inspect the rental listing: are there grammatical errors?
- Does the price seem too good to be true?
- Is the property listed on a free site?
- Are you being told you cannot see the property in person?
- Is there a screening process for you as a tenant?
- Are you being pressured to pay too quickly?

Be alert to the Microsoft SCAM!

Computer Software Service Fraud is on the rise. In one recent case a victim was using Google Maps on their computer when a pop-up claiming to be from Microsoft appeared on the screen - informing them due to unauthorised activity on their computer it had been blocked. The message advised not to turn off their computer and provided a phone number to call for further instructions.

Following a lengthy phone call with the fraudster, who provided them with a 'Microsoft code', they accessed the victims online banking and took them through a step-by-step process, resulting in two significant sums being transferred.

Fortunately on realising the fraud, the victim contacted their bank who were able to intercept the transactions and reimburse the loss. Whilst having their computer professionally cleaned software and files installed by the fraudster were found on the victim's computer.

Remember:

Fraudsters often use the names of well-known companies, such as Microsoft to commit their crime, as it makes their communication seem more legitimate. This is why it's important to think twice before giving out any personal information.

Only install software or grant remote access to your computer if you're asked by someone you know and trust, such as a friend or family member, and never as a result of an unsolicited call, browser pop up, or text message.

If you think you have downloaded a virus, consider having your computer looked at by a trusted technician in order to determine if malicious software was installed on your machine during the call.

Do you know what a money mule is?

Money mule activity refers to a money laundering process in which proceeds of crime are moved and transferred through personal and/or business bank accounts. Mule networks use collections of linked accounts to complete this process, allowing them to disguise the origin of criminally derived funds and extract them elsewhere.

Money mules have been found to be recruited from all age demographics but this is more prevalent between the ages of 17 and 24. The young person might have come into possessions such as luxury goods that they cannot account for. There might be evidence of them opening new bank accounts or using crypto exchanges with money they can't adequately explain the origin of.

Mules are often aware of the role that they are playing and do so for financial gain but there are times when the mule is tricked into performing this role.

How to protect yourself:

- Contact from someone you don't know trying to befriend you – particularly online and on social media platforms
- Job opportunities for quick and easy money / no experience required
- Deals that sound too good to be true
- Someone asking to transfer money to your bank account for you to pass on to

Case Study

Recently in Sussex a victim responded to an Instagram message from a well known celebrity account to assist with running their charity. Her role was to receive 'donations' into her own bank account and Paypal account where she then needed to move it into Crypotcurrency. As time went on she was asked to start sending her own money to people who were struggling financially. The victim ended up realising that the 'celebrity' was not real and had not been running a charity. She had likely been recruited as a money mule which ultimately resulted in her also being the victim of a fraud.