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
Antony Leadbeatter
Surrey Police &
Sussex Police
Economic Crime Unit

STAYING SAFE FROM SOFTWARE SERVICE SCAMS THIS CHRISTMAS

As we head into the festive season, many of us will unwrap new phones, tablets, laptops or smart home devices. While these gifts bring excitement and convenience, they can also attract the attention of criminals who use software service fraud to exploit unsuspecting users. Including fake security alerts and technical support calls, these scams continue to rise meaning that the period after Christmas, when new devices are being set up, is a prime time for offenders to strike.

Software service fraud typically involves someone pretending to be from a legitimate organisation, such as a well-known technology company, internet provider or security service. They may contact you by phone, email or pop-up message claiming your device has a virus or technical problem. Their goal is simple: to gain access to your device, steal personal information or convince you to pay for unnecessary or non-existent services.

This type of fraud can happen to anyone and here are some top tips to look out for:

Unexpected contact: Genuine companies do not cold-call customers to report technical issues. Treat unsolicited contact with caution, especially if they pressure you to act quickly.

Requests to install software: Fraudsters often ask victims to download remote-access programs. Never install software or grant access unless you are certain the request is legitimate.

More examples of service scams...

Demands for payment: Be wary of anyone asking for payment to fix a problem you didn't know you had. Reputable organisations will not demand upfront fees for unsolicited services.

Suspicious pop-ups: Fake warning messages can appear while browsing. Do not click on links or call phone numbers displayed in pop-ups claiming to detect viruses.

Check independently: If in doubt, contact the company using an official phone number or email address, sourced independently rather than from the message you received.

An elderly lady from Sussex who recently purchased a printer was subsequently defrauded out of £3,000 when fraudsters telephoned her offering support in setting up the printer and then gained access to her computer remotely. They set up payments from her accounts and installed malware onto her computer.

How to set up your device securely

As you enjoy your new gadgets, take time to set them up safely. Update the operating system, use strong and unique passwords, enable multi-factor authentication where possible and speak with family members (particularly those who may be more vulnerable) about the risks.

If you do encounter suspicious activity, report it. If you are elderly or vulnerable, please contact the police on 101.

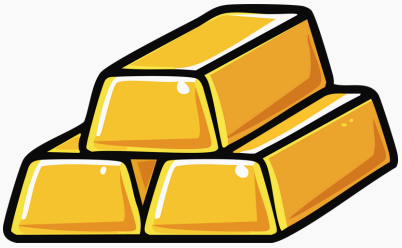
Stay informed, stay secure, and enjoy a safe and fraud-free Christmas.

Courier fraudsters requesting gold

Surrey Police and Sussex Police are currently seeing an increase in fraudsters who are calling victims purporting to be police officers, investigators or bank officials and requesting that victims purchase gold to assist with an "investigation". This gold is then handed over to a suspect posing as a "courier" who is working with the crime group. Fraudsters are providing victims with a fictitious story to tell the banks about why such purchases or withdrawals are being made, should they be asked.

Residents are being called and told:

- They must buy gold
- A courier will collect their card, cash, or gold
- Their bank account has been compromised
- Their card needs replacing
- A family member has been arrested



These are scams. The police will never ask for your financial details over the phone or send someone to collect your card, cash, or valuables.

Watch how this scam works: https://www.youtube.com/watch?v=mWCDpIvQuWg

HIS MAJESTY'S REVENUE AND CUSTOMS (HMRC) PHISHING SCAMS

As we approach the deadline to submit self-assessment tax returns to His Majesty's Revenue and Customs (HMRC) on 31January we anticipate there may be an increase in fraud reports involving people impersonating HMRC via calls and phishing text and WhatsApp messages. We advise not to engage with these contact attempts and if in doubt to contact HMRC directly. This can be done online here: https://www.gov.uk/log-in-register-hmrc-online-services. Alternatively, you can contact them on 0300 200 3311.

Recently a female student from Surrey, in her 20s received an automated phone call purporting to be from HMRC regarding outstanding tax owed, and to press one to speak to an agent.

She was transferred to a female who stated that she owed money in tax. The female student explained that she did not believe she needed to pay anything, however the caller disagreed and stated a tax expert will call back and explain what was owed.

A call was received within minutes from a male claiming to be from HMRC appeals division and that failure to pay tax will result in arrest and court action. He claimed she owed £3,000, but a payment of £2,200 would settle the matter. The male asked for payment via a money transfer service. After payment was made, an HMRC letter was sent via WhatsApp to the victim confirming that she owed the amount just paid.

A young female from Sussex in her 20s received a call on her mobile from someone claiming to be from HMRC and stated that she owed tax. The callers stated failure to pay would lead to her being arrested.

Out of fear of arrest, she paid £300 via a money transfer app as directed by the caller, but they then demanded more money and became more threatening. She began to suspect this was a scam and ended the call and spoke to her mother who advised to report the matter to the police.

If you suspect that you have been a victim to an HMRC scam, we advise you to report to this to Report Fraud via https://www.reportfraud.police.uk/ and your bank who may be able to recover the money you have sent.