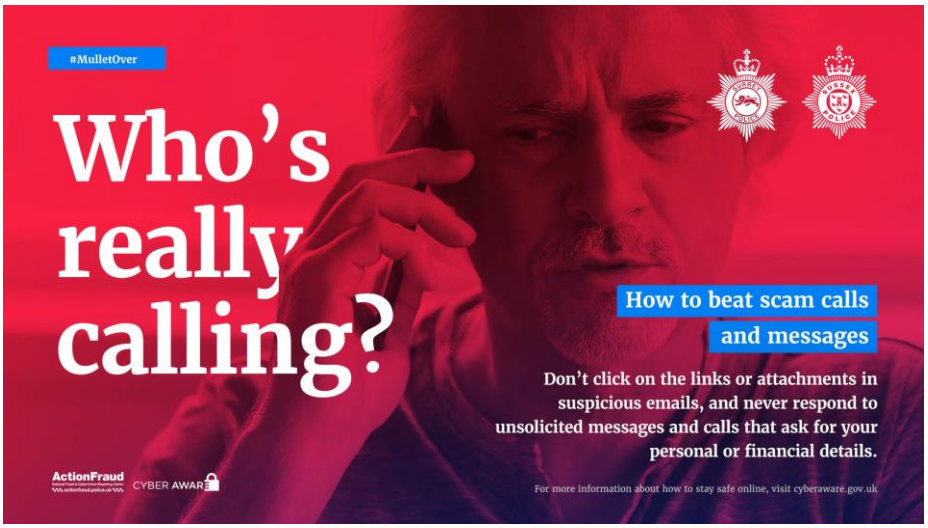
Keep your money safe

Surrey and Sussex Police Fraud Newsletter July 2019

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 Andy Richardson, Surrey & Sussex Police Economic Crime Unit.

How to beat 'phishing' messages and calls



Last month, our forces supported a national campaign to make people aware of 'phishing', whereby criminals make contact, generally by unsolicited text, email or call, and attempt to trick us into revealing personal and financial information. That information can then be used to commit fraud and cybercrime. From emails and text messages asking you to "verify" account details or from HMRC saying you owe tax money, to cold callers claiming to be from your bank or the most commonly impersonated brand – TV Licensing - a phishing message is designed to look and feel authentic.

The good news is some simple advice can help you protect yourself from most phishing attacks:

- Don't click on the links or attachments in suspicious or unexpected emails
- Never respond to unsolicited messages and calls that ask for your personal or financial details.

Keep your money safe

- If you think the communication might be genuine, you can check by contacting the company directly using contact details you know to be correct, such as the phone number on official correspondence, and not the contact information provided in the message.
- Even if an email or letter is personally addressed to you by name, or if a call looks like it comes from a genuine phone number please think twice. Fraudsters are now spoofing genuine phone numbers.

Seagulls in chimneys and slow internet scams

Sadly we continue to see cases where the most vulnerable members of our communities are targeted by ruthless criminals.

In East Sussex, a man knocked on a woman's door and said he'd seen a trapped seagull in her chimney. The fraudster sent his 'apprentice' into the victim's loft and the apprentice reported that the seagull had gone but the roof now needed emergency repairs. The victim felt overwhelmed by the men in her home. She gave the fraudster £800 cash to repair the damage and was told to keep their deal a secret from her neighbours.

When the man phoned the next day requesting more money for materials, the victim grew suspicious. The fraudster offered another builder's name and number for a second opinion but by now the victim had realised this was a scam.

In North Surrey, a victim was phoned by a man pretending to be from BT. He was calling to offer her £400 compensation for the slow speed of her internet. The man then said he had sent £1000 to the victim by accident instead of £400. He gained access to her computer and her online banking account, then asked her to transfer him the £600 difference whilst he updated her internet. The victim became suspicious and phoned her bank at the same time. Thankfully her bank explained this was a scam and told her to hang up immediately.

While the details of these cases are very different, there are similarities in how scammers operate:

- Whether it's an example like the roof damage story above, or whether you've met someone through online dating, if you're told to keep something secret from friends, relatives or neighbours, that's a huge warning sign that things are not above board.
- Fraudsters will often offer you a way to check they are legitimate – whether that's a second opinion, or the option of talking to one of their colleagues to verify their identity. Do exactly as the person in the BT scam did: call to check, on another phone line, and using a phone number you know to be correct.

Both of the people in our cases became suspicious, trusted their instincts and would not let the scammers go further. We always say that if something feels wrong to you, or feels too good to be true, it often is. Do not be afraid to hang up on scammers.

Keep your money safe

Courier fraud rise in Surrey

Last month there was a rise in courier frauds (where ‘couriers’ are sent to homes to collect money or bank cards after fraudsters have made contact and persuaded the victim they need their money or bank card for a seemingly legitimate reason) in Surrey. This is a heartless crime with the oldest victim last month being 96 years old, and the average loss being £2000. Requesting bank cards are provided is the most frequent scenario we are seeing.

Through Operation Signature, our activity to protect vulnerable and elderly people from fraud, we’re able to ensure as far as possible that people do not become repeat victims of this callous crime, but you can help us stop it happening in the first place. The police and your bank will never contact you out of the blue and ask for your bank details, PIN, money or cards, and we’ll never send someone to your house to collect things like this, and you should hang up on anyone who asks you to do this. Please tell anyone you think needs to know this; even write a reminder by the phone if that will help.

How you can help us

If you or someone you know is vulnerable and has been a victim of fraud call:

Surrey Police on 101 or visit www.surrey.police.uk
Sussex Police on 101 or visit www.sussex.police.uk

Report fraud or attempted fraud, by contacting Action Fraud at http://www.actionfraud.police.uk/report_fraud or call 0300 123 2040