Keep your money safe

Surrey and Sussex Police Fraud Newsletter October 2018

Each month, we see many incidents of fraudsters targeting our residents in an attempt to defraud them. Operation Signature is our answer to preventing and supporting 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

What is number spoofing?

Fraudsters can now send you a scam text displaying a phone number or name that looks like one you already recognise.

An elderly man in East Sussex received a text message from PayPal stating that his account had been frozen due to suspicious activity. In order to get the account back, he had to click on a link sent with the text within 36 hours. This link then took him to what appeared to be an official PayPal website which asked for his card details.

The victim then received a phone call from the 'NatWest Customer Service' – the same number that is printed on the back of his bank card. A fraudster informed him about a suspicious transaction from his account in Manchester for £400 and that in order to re-establish his account he would need to give his bank details.

Two days later he discovered that funds had been transferred from his multiple bank accounts into his current account and £20,000 of this had been transferred out.
Then Natwest were in contact with him regarding overdraft charges and it became clear that the funds had not been transferred by them or the victim but by a third party posing as the bank.

The victim's accounts were frozen by Natwest but the fraudsters had managed to clone the bank's actual customer service phone number and made it look legitimate.

Keep your money safe

Signs of scam calls

Never assume that someone is who they say they are just because their number matches that of an organisation you know.

In fact, if someone tries to draw your attention to the number on your caller ID display, you should immediately become suspicious.

Never give anyone your four digit PIN, your full online banking passwords, to transfer or withdraw money, or to give your card to a courier. Your bank or the police will never ask you for this information.

Your bank will 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.

Fake calls from 'Virgin Media'

In Woking, Police were called by bank staff at NatWest about a 65 year old woman in the branch; who stated that Virgin Media called her asking her to provide them with £4000.00 and to leave a box in a safe place so Virgin Media could collect it.

This situation began with a telephone call from a fraudster saying the woman's internet account had been hacked she had to sort the problems out. The woman was then transferred through to 'Virgin Media' and kept on the phone for 45 minutes to discuss her internet router.

Another call followed from a 'call handler' who said she'd receive £500 worth of compensation due to her computer being hacked in June. During this time the caller controlled the victim's computer. She was then directed to go to her bank and withdraw £4500, asked to put it in a shoe box and then take it to the post office. The victim then went to her bank who called police. The fraudsters also had hacked into her online banking account where they transferred £5000.00 from her savings account into her current account.

If you suspect someone you know may be vulnerable to fraud, please share this newsletter with them and encourage them to look at the 'Little Book of Scams', available on the following link: http://tinyurl.com/z8khtgh

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 www.actionfraud.police.uk/report_fraud or call 0300 123 2040.

Subscribe for the newsletter at commsrequests@sussex.pnn.police.uk