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 Rob Walker, Surrey & Sussex Police Economic Crime Unit

Lottery scams

"If it sounds too good to be true.....it probably is"

A female victim from East Surrey received a call from someone claiming to be from the Postcode Lottery team.

The caller informed the victim she had won a voucher and a free holiday. The caller then asked the victim to provide her personal details so that her prize could be registered.

Thankfully the victim felt this suspicious and did not pass over any details. The victim later confirmed with the Postcode Lottery that it was in fact a scam.

How to protect yourself:

- *Never respond to communications suggesting you are a winner. If you haven't entered a lottery then you can't have won it!*
- *Never disclose your banking or information or pay fees in advance*
- *Do not click links in unsolicited emails or messages, even if they company name and logo looks genuine*
- *Verify the identity of contact by calling the genuine organisation or person, do not use the contact methods provided in suspicious emails or messages*

Computer Software Service Scams

Have you been contacted by someone out of the blue claiming you have a computer problem? Have they told you your broadband speed is slow and you are due a refund? Are they claiming you have been hacked and they need to support you?

Sussex and Surrey police have seen reports of victims receiving telephone calls and computer pop ups in regards to them requiring software support on their devices or broadband. Fraudsters will often use the name of genuine providers such as BT, Microsoft, Amazon or Sky to make victim's believe the contact is from a genuine company.

Case Study

A 64 year old Female in Sussex was using her computer when her computer crashed and a pop up appeared suggesting she call a number for support. The victim called the number provided and was told if she paid £100 the IT support company would fix her issues.
The victim paid this amount and all appeared to be 'fixed' whilst the IT support had access to her laptop.

A few days later the victim had issues again when using her laptop to purchase a product online. This time the victim has pornography images flash on her screen. The victim received a call from the supposed IT support company who claimed she had been hacked and needed to pay a further £800 to fix the issue. The victim was instructed to send this via PayPal which she questioned but the caller insisted PayPal was the best payment method.

The victim unfortunately paid this second amount and soon after realised she had been a victim of fraud.

Protect yourself from computer scams

- **If you receive a call like this hang up. 'Take Five' and verify via a trusted method.**
- **Never allow anyone to remotely access your devices**
- **Do not download software at the request of a caller**
- **A genuine provider will never call you out of the blue regarding issues with your devices or broadband**

If you are having issues with a device or broadband, contact your provider or the retailer you purchased from.

Email and social media account hacking

Sussex and Surrey police have seen several reports of victims emails and social media accounts being hacked and used by scammers to gain money from friends and family.

In one case, an 85 year old, female Surrey resident received an email from who she thought was her friend. The victim was being asked to purchase two Google play cards on her 'friends' behalf for her niece's birthday. The victim agreed to do as instructed and brought two Google play vouchers, sending a picture of both to the fraudster. The victim was then told the codes were not working and instructed to purchase another £600 worth of vouchers. The victim again agreed to do so, thinking she was helping her friend and sent over images of the voucher codes.

After reporting suspicions to her local supermarket where she purchased the vouchers it was confirmed the 'friends' email had been hacked and the victim had sent the voucher codes to a fraudster. In this incident, the victim thought the sender to be her friend as the language used in the email was just as her friend was usually write. Scammers are very clever and will try to make messages look as genuine as possible.

How to protect yourself

- **Have strong passwords for all accounts**
- **Do not click on links and attachments unless you can verify where they have come from**
- **Always ensure your devices have Anti-virus and are regularly updated**
- **Be cautious when using public WIFI**
- **Enable two-factor authentication**

Always verify with friends, family and colleagues if the request they have sent is genuine. Could you call them to confirm or contact them on a different platform?

What to do if your account has been hacked?

- *Change your passwords*
- *If you cannot access your account, contact your provider through their 'help' or 'support' pages to recover your account*
- *Set up two –factor authentication*
- *Notify your friends, family and contacts*
- *Check your email filters and forwarding rules , a common trick fraudsters use is to have messages forwarded to a new account they can access*

Have you been a victim of fraud?

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.