JANUARY 2024

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

VIRGIN MEDIA - COMPUTER SOFTWARE SERVICE FRAUD

Several reports have been received in the past month as a result of fraudulent Virgin Media contact. A resident in Sussex reported that they had received a call from a suspect purporting to be from Virgin Media.

The suspect knew details about his Virgin Media account including their previous bill amount, and router ID. They were instructed to download software onto their iPhone. The suspect then logged onto the PC via teams and remotely controlled it. The suspect also told the male to provide them with the codes that they had received in order for them to log into the would-be victim's bank account.

Thankfully at this point they realised it was a scam and ceased to engage before any money was taken. They contacted Virgin Media who confirmed that it was a scam.

An elderly female in Camberley reported losing £370 to a fraudster posing as Virgin Media offering to provide them with a refund to compensate for poor service. She was instructed to download an app onto her phone to enable the refund, but instead of receiving compensation the money was actually removed from her own bank account.

What to do if you think you've given remote access to a scammer

- Switch off both the device and your wi-fi connectivity.
- Speak to your bank as a matter of urgency.
- Remove the relevant app from your list of recent downloads or installed programs, check for other programs that may have been installed remotely.
- Change your email and online banking passwords and, where possible, enable two-factor authentication.
- If you have security software, ensure it has all new and recent updates – then run a full security scan.

Braille Scam Books

⠺⠕⠗⠇⠙
⠃⠗⠁⠊⠇⠇⠑
⠙⠁⠽

Sussex Police & Surrey Police marked World Braille Day on 4 January with the release of a braille version of 'The Little Book of Big Scams V5'. World Braille Day is an international day celebrating the importance of braille as a means of communication for blind and visually impaired people.

The Little Book of Big Scams is a booklet we have used extensively in previous editions within the community and with vulnerable fraud victims and until now, the sight impaired community were unable to access this excellent product- The Little Book of Big Scams – 5th Edition (sussex.police.uk)

We are delighted to be able to now provide these to those who will benefit from this product and are working with our Neighbourhood teams, Victim Fraud caseworkers and local sight-loss and blindness charities to make this widely available within our two force areas.

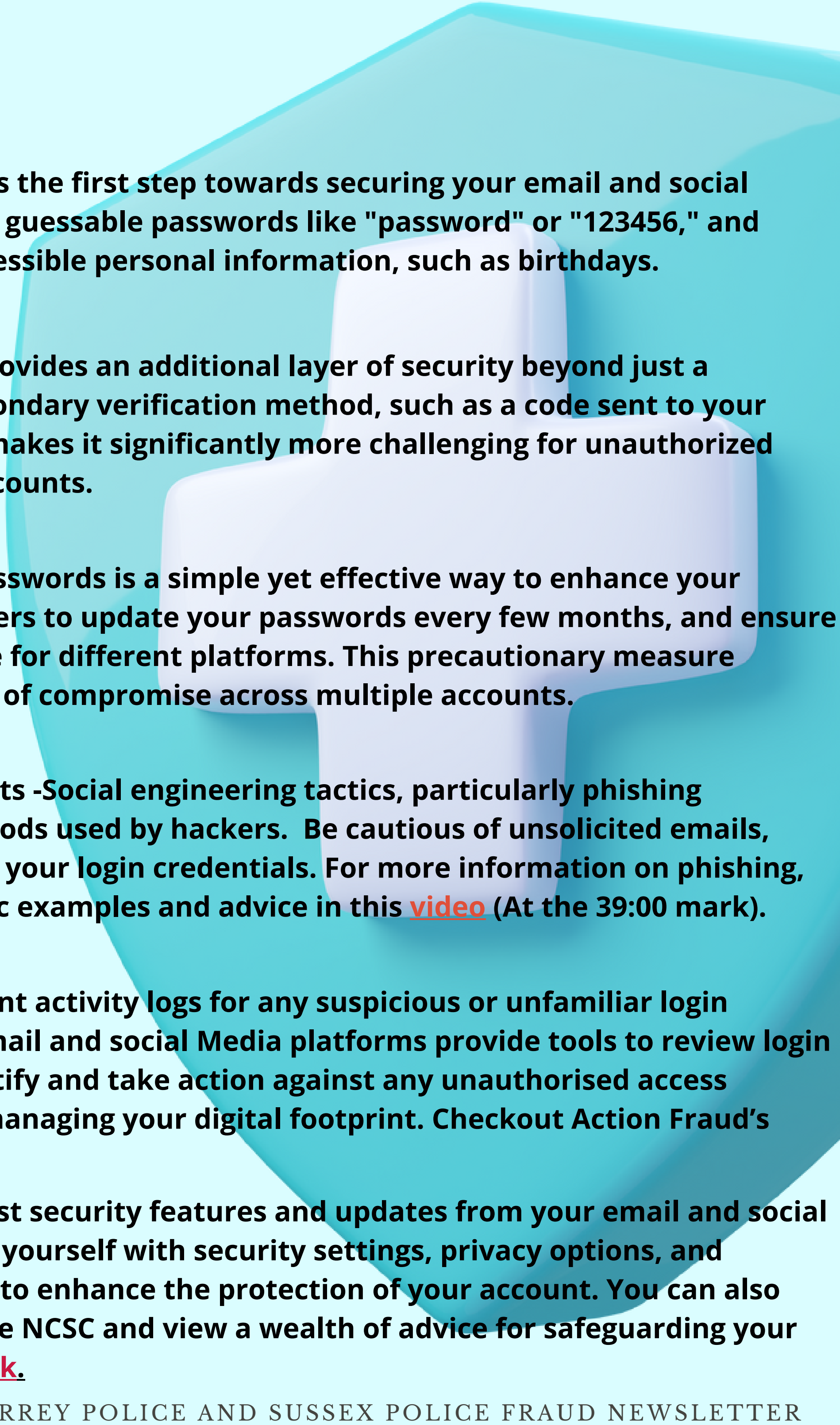
Bernadette Lawrie BEM the Financial Abuse Safeguarding Officer for Sussex and Surrey Police said "Educating people on the signs to look out for relating to fraud and providing tips on how best to protect yourselves is essential to reduce revictimisation and limit financial loss. With fraud being responsible for nearly half of all reported crime, we are so pleased to have been able to make this product accessible to the visually impaired."

For more information on how your organisation can access this product please email: operation.signature@sussex.police.uk

EMAIL AND SOCIAL MEDIA ACCOUNT TAKEOVERS

In an era dominated by digital connections, our email and social media accounts are often integral aspects of our personal and professional lives. However, with great connectivity comes great responsibility. Email and social media account takeovers are one of the most common crime types our Cyber Crime Unit deals with.

PROTECT PROTECT PROTECT...



...BUT HOW?

☑ Creating a robust password is the first step towards securing your email and social media accounts. Avoid easily guessable passwords like "password" or "123456," and refrain from using easily accessible personal information, such as birthdays.

☑ Two-factor authentication provides an additional layer of security beyond just a password. By requiring a secondary verification method, such as a code sent to your mobile device or email, 2FA makes it significantly more challenging for unauthorized individuals to access your accounts.

☑ Frequently changing your passwords is a simple yet effective way to enhance your account security. Set reminders to update your passwords every few months, and ensure that each password is unique for different platforms. This precautionary measure significantly reduces the risk of compromise across multiple accounts.

☑ Be aware of phishing attempts -Social engineering tactics, particularly phishing attempts, are common methods used by hackers. Be cautious of unsolicited emails, messages, or links asking for your login credentials. For more information on phishing, we run through some specific examples and advice in this video (At the 39:00 mark).

☑ Frequently check your account activity logs for any suspicious or unfamiliar login locations or devices. Most email and social Media platforms provide tools to review login history, allowing you to identify and take action against any unauthorised access promptly. It's also good for managing your digital footprint. Checkout Action Fraud's video on this here.

☑ Stay informed about the latest security features and updates from your email and social media platforms. Familiarise yourself with security settings, privacy options, and additional features provided to enhance the protection of your account. You can also report malicious emails to the NCSC and view a wealth of advice for safeguarding your online accounts using this link.