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

KEEP CRIMINALS OUT WITH 2-STEP VERIFICATION (2SV) – EVEN IF THEY KNOW YOUR PASSWORD

Turning on 2SV gives your most important accounts an extra level of protection, especially your email. It can be turned on in a matter of minutes – time well spent to keep the fraudsters out.

WHAT WE ARE DOING IN THE COMMUNITY

Police took to the streets of Guildford, on Monday, 17 April as part of a national day of action, to raise awareness with the residents of 2SV also known as 2 Factor Authentication (2FA).

The team, which included local and regional representatives, spoke with commuters at Guildford train station about the importance of having the security process in place on their online platforms. They then went into Guildford town centre and were invited into Barclays Bank to provide the information to their customers, engaging with them inside and with other members of the community outside the branch.

HELPFUL FRAUD PREVENTION LITERATURE WAS ALSO SHARED WITH OTHER BANKING ORGANISATIONS.

HOW TO SET UP 2-STEP VERIFICATION

2SV can usually be found in the security settings of your account. Sometimes it's called 2-factor authentication (2FA) or multi-factor authentication (MFA). It is available for most of the major online services, such as email, banking, and social media.

WHY SHOULD I SET UP 2-STEP VERIFICATION?

By setting up 2SV, it can help protect you from cyber criminals as it asks for more information to prove your identity when you log in to your online accounts.

It provides a way of 'double checking' that you really are the person you are claiming to be when you log in so creates double the work for criminals trying to access your online accounts, even if they know your password.

Even if you've always looked after your passwords, they can still be stolen through no fault of your own – it's easier than you think for someone to steal your password.

When you turn on 2SV, you will be asked to provide a 'second step', which is something that you (and only you) can access. This could be a code that's sent to you by text message or created by an app.

You may also be able to use your fingerprint, facial recognition, or memorable information. You don't necessarily need a mobile to turn on 2SV. Some providers will let you use a landline number, or a separate device, such as a card reader or USB stick.

We recommend turning on 2SV for your email and social media accounts, as well as any accounts that contain lots of personal or sensitive information. Often online banking has 2SV enabled by default but do double check if you are unsure.

Take a few minutes to secure your online accounts now.

FINANCIAL ABUSE BY A KNOWN PERSON

As people age their need to rely on others for support can increase, whether that is through personal care needs, day-to-day tasks or financial affairs. Financial abuse can take many forms, including abuse by a position of trust and sadly can be perpetrated by someone close to you.

Friends, family members, carers or company employees may be asked to look after your personal or business finances. They may instead take advantage of their access to bank accounts or information for their own benefit or misuse the assets of a business to embezzle funds for themselves.

In 2024, Sussex Police received 224 reports of financial abuse by suspects known to the victims with Surrey Police receiving 112 reports for the same period. These reports accounted for a combined loss of over £13 million pounds, with almost half of these cases relating to victims over 75 years old.

Older people can be an unfortunate target of this crime type, due to being in receipt of pensions and due to the higher value of assets they may have built up, by comparison to younger age groups.

Reporting a fraud by a person known to you can be increasingly difficult if the suspect is a family member, carer, or friend as there may not be an alternative support network outside the influence of the suspect. There can also be the risk and/or fear of retaliation or further victimisation which can inhibit reporting.

In a recent example, a housebound man in poor health from Sussex, was financially abused by a member of his own family. They had offered to do his shopping for him, which the man agreed to, and gave the relative his bank card and PIN number.

Eventually this came to police attention when he had fallen behind on his rent, had very little food in the house and insufficient funds to pay his bills.

It transpired that an additional £8,000 had been taken from his account, by the relative, without his knowledge.

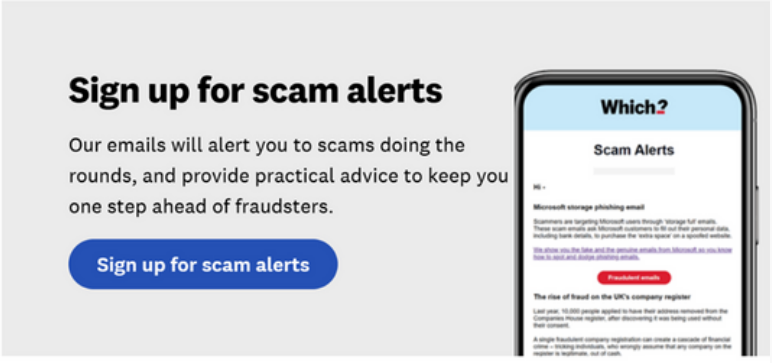
In a similar case in Surrey, an elderly female had sought the support of a close friend to buy her groceries using her bank card (having also shared her PIN). After six months, it was discovered that £3,000 had been taken from her account unlawfully and welfare concerns were made regarding the lack of money she had left to pay her utility bills.

This fraud type when perpetrated by a family member or friend is a betrayal that can have devastating effects on the victim.

If you have been given a position of trust, it is your responsibility to keep a close eye on the individual's finances, particularly if they are vulnerable. Handle bills and statements with care and shred them before throwing them out.

If you are concerned that a vulnerable person in your area is being financially abused by someone they know, report your concerns to Sussex Police or Surrey Police on 101.

SIGN UP FOR THE WHICH ? FREE – SCAMS ALERTS SERVICE



Their emails will alert you to scams doing the rounds and provide practice advice to keep you one step ahead of fraudsters.

Sign up with the link - https://signup.which.co.uk/wlp-scamalert-newsletter