Keep Your Money Safe

Surrey Police and Sussex Police Fraud Newsletter

In this issue:

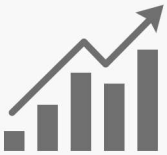
"Each month we see many incidents of fraudsters targeting our residents in an attempt to defraud them. We're working hard to prevent this and support vulnerable victims of fraud or scams. By following our tips and encouraging family, friends and colleagues to do so too, you can reduce the risk of becoming a victim."

Detective Chief Inspector
Antony Leadbeatter
Surrey Police &
Sussex Police
Economic Crime Unit

SOCIAL MEDIA HACKING: A GROWING THREAT

In today's digital age, social media is more than just a place to stay connected — it's a vital part of our daily lives. From sharing family updates to managing small businesses, platforms like Facebook, Instagram, WhatsApp, and TikTok are embedded in how we interact. Unfortunately, this reliance can also make us vulnerable.

Social media hacking is on the rise, and fraudsters are becoming increasingly sophisticated in how they exploit both individuals and organisations. Sussex Police and Surrey Police are receiving a growing number of reports from residents each month related to hacked accounts, online impersonation, and fraud committed through compromised profiles.



HOW DO SOCIAL MEDIA HACKS BEGIN?

Most social media hacks begin with phishing attempts. These are deceptive messages that convince you to click a link or enter login details on fake websites that look legitimate. Once a hacker has your login information, they may:

- **Change your password and lock you out of your account**
- **Message your friends and followers to ask for money or personal details**
- **Post harmful or offensive content**
- **Use your account to spread malware or phishing links**
- **Target connected business pages or other linked accounts**

We're also seeing an increase in social engineering, where criminals gain access through conversation, often by pretending to be a friend or support representative. In some cases, users can be convinced into handing over two-factor authentication (2FA) codes, thinking it's part of a security check.

EXAMPLE

These two recent examples of social media hacking reports from Sussex and Surrey show how everyday users are targeted.

A victim from Sussex reported receiving a message from their sister on WhatsApp requesting money. Unfortunately she sent the money before verifying that her sisters WhatsApp account had actually been hacked. The money, almost £500 was sent via a code to a recipient in Africa.

A lady from Guildford received a direct message on Instagram from someone she believed was a friend, claiming their account had been hacked and requesting a code to regain access. She received a code and sent it on via Instagram. She was immediately logged out of her account and then received multiple messages asking if she wanted her Instagram account back. Despite not responding she found she no longer had access to her account and noticed that several unfamiliar email addresses had been linked to it. She then received a notification from Instagram warning there had been multiple login attempts to her account.

Stay Safe: Practical Tips to Protect Your Social Media Accounts

Protecting your social media presence doesn't need to be over complicated. A few good habits can go a long way in keeping your accounts secure:

Use Strong, Unique Passwords

- Avoid using the same password across multiple accounts.
- Use three random words
- Consider using a password manager to generate and store complex passwords.

Enable Two-Factor Authentication (2FA)

- 2FA adds an extra layer of security by requiring a code sent to your phone or email.
- Turn this on for all major platforms (Facebook, Instagram, WhatsApp, etc.).

Be Wary of Suspicious Messages

- Never click on unexpected links, even if they appear to come from friends.
- Look out for strange language or urgent requests

Check for Impersonation

- Regularly search your name to see if fake accounts are pretending to be you.
- Report any impersonation directly to the social media platform.

Keep Your Apps & Devices Updated

- Always install the latest updates to patch known security vulnerabilities.
- Enable automatic updates where possible.

WORLD ROMANCE FRAUD AWARENESS DAY

Sussex Police and Surrey Police are supporting a national initiative to tackle romance fraud, coinciding with World Romance Scam Prevention Day on 3 October. Officers and partner agencies will be engaging in public events across the region to raise awareness and help prevent these heartless crimes.

Romance fraud is a growing issue where criminals exploit individuals emotionally in order to steal money. These scams often begin innocently on dating apps, social media, or even gaming platforms, but can quickly escalate once trust is established.

Recent local examples highlight the tactics used:

A woman in her 40s from Sussex, who was caring for an elderly relative, was contacted via a popular gaming app. The conversation quickly moved to Telegram (a cloud based messaging service), where the fraudster began requesting money in the form of gift cards. This raised the victim's suspicions and, recognising the red flags, she ended contact, thankfully before any loss occurred.

In Surrey, a man was contacted through a dating app but was soon encouraged to move the conversation to WhatsApp. The fraudster refused to meet in person unless he sent a substantial amount of iTunes vouchers. When the man travelled to the location she claimed to live and found further evasiveness, he reported the incident to local police.

These cases underline the importance of staying vigilant when forming online relationships. Fraudsters are skilled manipulators and often target people at vulnerable times in their lives.

TOP TIPS ON HOW TO STAY SAFE FROM ROMANCE FRAUD

Don’t rush into online relationships - Take your time. Get to know the person, not just the profile.

Analyse their profile: Look closely. Protect yourself by verifying who they really are.

Talk to your friends and family - Be wary of anyone who tells you to keep the relationship a secret.

Evade scams - Never send money or share bank/personal details with someone you've only met online.

Stay on the dating site’s messaging service - Fraudsters often encourage victims to move to private messaging apps to avoid detection.