Keep Your Money Safe

Surrey Police and Sussex Police Fraud Newsletter

In this issue:

Online safety

Common scams

Top tips

Websites that can help

Gift card fraud

Lived experiences

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

ONLINE SAFETY FOR THE NEW SCHOOL YEAR

As the new school year begins, Sussex Police and Surrey Police would like to remind parents, grandparents and carers, of the importance of keeping young people safe online. While digital platforms offer educational and social benefits, they also expose children and teens to a range of serious risks.

Two key threats currently targeting young people are sextortion and money muling.

Sextortion involves criminals manipulating or coercing young people into sharing explicit images or videos, then threatening to share the content unless a ransom is paid. This type of blackmail can have devastating emotional and psychological effects.

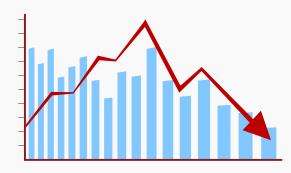


Learn more here:

https://www.actionfraud.police.uk/a-z-of-fraud/sextortion

Money muling occurs when young people are tricked or recruited - often through social media - into moving stolen money through their own bank accounts. Even if they believe they're helping someone out or earning "easy money", this is a serious criminal offence.

Details can be found here: https://www.nationalcrimeagency.gov.uk/moneymuling.



Another growing concern is investment fraud, particularly involving cryptocurrency. Scammers often target younger users with offers that appear to promise fast profits. These can quickly result in significant financial loss and identity theft. For warning signs and advice please visit: https://www.actionfraud.police.uk/cryptocurrencyfraud

Start the conversation early - and keep it going

Ask your child to walk you through the games they play, the sites they visit, or the videos they love. Talk openly about common online risks like oversharing, inappropriate content, cyberbullying, and interacting with strangers. Stay informed about the latest trends and lead by example with your own digital habits.



Point them in a safer direction

Encourage the use of child-friendly apps and platforms, such as YouTube Kids. Check in regularly on what they're watching and sharing, especially on sites like YouTube and TikTok.

Keep up with digital trends - especially the risky ones

Some games and social platforms have raised concerns for promoting violence, gambling, or unmoderated messaging. Get to know which ones your child is using and how they work.

Don't underestimate the emotional impact

Social media and messaging apps can be powerful - sometimes overwhelmingly so. Help your child understand how online experiences can influence emotions, self-esteem, and mental health.

Respect age restrictions - they exist for a reason

Most platforms have age limits to help protect children. Stick to them and talk to your child about why they matter.

Set clear rules from the beginning

Agree on boundaries together: what's OK to do online, how long to spend on devices, and how to treat others with respect. Kids need structure and support to make smart choices online.

Make the most of built-in tools

Use parental controls on devices, games, browsers, and social platforms. Enable privacy settings, safe search features, and family filters from your internet provider. These tools add an extra layer of protection.

Be cautious with video calls

Always update apps to their latest version and adjust settings to ensure calls are private and secure. Allow communication only with trusted contacts.

Talk about online gaming

Gaming can help kids with creativity and problem-solving - but it can also expose them to strangers, pressure to spend money, or risky behaviours. Make time to chat about the games they play and how they use them.

Remind them to think before they share

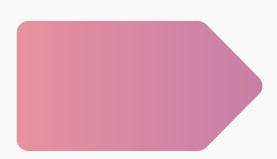
Personal details, photos, videos - once they're online, they can be hard to take back. Talk to your child about what's appropriate to post and how to protect their and others' privacy.

Stick to trusted sources for apps

Download apps only from official stores like Google Play or the App Store. Where possible, use your own email address when creating accounts for your child.

Stay observant, not overbearing

Keep an eye on your child's online behaviour and watch for warning signs. Sadly, some young people have been targeted for serious online threats from scams and grooming to involvement in criminal activity.



Organisations that can support you

Get Safe Online

https://www.getsafeonline.org/safehappykidsonline/

Child Exploitation and Online Protection (CEOP) https://www.ceop.police.uk/safety-centre/

Internet Matters

https://www.internetmatters.org



GIFT CARDS USED IN FRAUD



Since the start of the year, in Sussex and Surrey we have received 170 reports of gift cards being used in fraud scams, impacting victims of all ages with over $\mathfrak{L}1.1$ million pounds lost. We have found gift cards being used as a payment method, in several types of frauds including hacking and sextortion, phishing, online shopping, investment, romance and employment fraud.

Last month, an elderly gentleman from Surrey was subject of a 'fraud recovery' fraud. Having been a victim of investment fraud previously, he was contacted by email with a claim that he was due a large payment due to the lost money being traced. To obtain this money, he was asked to send money via Amazon gift cards by taking photos of the redemption code and sending these to the scammer. After each redemption code was sent, more money was then requested with the promise of recouping his lost funds. In total he sent over £15,000 in vouchers leaving him in a desperate financial state.

A Sussex teenager was on a dating website and matched with another person. They started talking to each other and after a while moved the conversation over to the social media app Telegram. After chatting for a few days, they swapped explicit photos of each other. Immediately after this, he received a threatening message requesting a payment of £200 via Apple gift cards or they would share the photos with his Instagram friends. Fearing this, he sent £200 in Apple vouchers. Straightaway, a further demand was made for more money, which again he sent. After this he blocked all contact with the suspect and set his Instagram profile to private.

In July, a lady in her 70s reported that she had been victim of a romance fraud. Three years ago she started following the actor Johnny Depp on Instagram. Soon afterwards, she received a personal message on Instagram by someone impersonating the famous actor.

Over the next three years, believing she was in a romantic relationship with Mr Depp, she would send money in the form of Apple vouchers, to pay for things including a new computer on his request. In return she would receive the occasional gift in the post. During this time, she sent approximately $\mathfrak{L}9,000$ worth of gift card voucher codes to the suspect who was impersonating the celebrity. Using gift cards to make payments is becoming an increasingly common strategy for criminals as it is less likely to be intercepted and are difficult to trace compared to bank transfers.

If you feel you have become victim of a crime involving gift cards, please report this to Action Fraud on the <u>following link</u> or call 0300 123 2040. Alternatively, if you are elderly or vulnerable you can report this to Sussex or Surrey Police by calling 101. https://www.actionfraud.police.uk/

If you have sent Apple gift cards, please visit the <u>following webpage</u> at Apple for support and to report this: <u>https://support.apple.com/en-gb/120933</u>

If you have sent Amazon gift cards, please visit the <u>following webpage</u> at Amazon for support and to report this:

https://www.amazon.co.uk/gp/help/customer/display.html? ref =hp gcs csd d2 other 1 GGKDN3QZSKBFGNBF TUgYdY7376&nodeld=GGKDN3 QZSKBFGNBF&gid=1754992858091&sr=1