

# Keep Your Money Safe



*Surrey Police and Sussex Police Fraud Newsletter*

## *In this issue*

Your Digital Footprint

What Goes Online Stays Online

Celebrity Fans...Who are you really following?

Case Study

How Safe are your School's Finances?

Case Study

"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

## Your Digital Footprint

Every time you visit a website, send or receive a message or email, buy or book anything online, comment on a post, upload a photo or find directions on your phone, you're adding to your digital footprint. When you stream music, make a video call or use a smart speaker, that adds to your digital footprint too.

### What goes online stays online:

- Think twice before sharing information about yourself, family members or friends that would be better kept private. That goes for social media, forms on websites and apps, responding to texts and messages and when taking part in surveys and quizzes.
- Think before you post. Even if your social media privacy settings are set up correctly, there's no guarantee that your posts or photos won't be shared beyond those who you want to see them.
- Be aware that every time you visit a website, your activity is visible to tech companies like website owners, browsers and search engines.

For more information visit [www.getsafeonline.org/digitalfootprint](http://www.getsafeonline.org/digitalfootprint)

Remember: Every time you do something online, you add to your digital footprint - the impression you create on the internet through your online activity.

We've all heard the expression 'what goes online, stays online' so do you ever think about exactly what you're doing online, who might see it and what they could do with it?

# Celebrity Fans...Who are you really following?

More and more victims are losing money to 'famous person' scams. In Sussex and Surrey we have seen examples of fraudsters posing as the money expert Martin Lewis, appearing to endorse investment opportunities and get rich quick schemes.

An increasing number of romance frauds have been reported locally where individuals believe they are chatting directly with celebrities. These have included the actor Russell Crowe, singers Michael Ball and George Ezra and even the super vet Noel Fitzpatrick citing cash flow problems.

Contact is typically instigated through social media channels with money being requested soon after the chat has moved to a less public forum or direct messaging. Reasons for the need for money range from the plausible to the extreme and victims are generally paying through the purchase of Amazon or Steam vouchers.

## Case Study

A female in her 50's from Surrey, was on a Facebook group for fans of the famous Croatian Cellist HAUSER. Believing it was him she was messaging directly, their contact moved off the Facebook group (which has since been deleted) and they continued to swap messages on WhatsApp.

The conversation became romantic and soon afterwards the requests for money started to come, with the HAUSER impersonator claiming he was on a world tour and needed the money to get out of his contract. She lost £1250 over a month to this fraud.

If you have any doubts about an email message received, contact the organisation directly. Do not use the numbers or address in the message – use the details from their official website. If you have received a suspicious email, forward it onto the suspicious email reporting service: [report@phishing.gov.uk](mailto:report@phishing.gov.uk)



## How safe are your local school's finances?



Whilst we do not want to deter you from putting trust in your local schools, we cannot ignore the fact that these kind of offences do occur within all establishments.

In some cases, individuals take advantage of the responsibility given to them, and that is exactly what 61-year-old Debra Poole did for almost a decade.

### Case Study

In March of this year, a former school business manager who stole hundreds of thousands of pounds from her employer was sentenced to six and a half years behind bars when she appeared at Kingston Crown Court.

Debra Poole, who was the School Business Manager for Hinchley Wood Primary School in Esher, was in charge of the school bank accounts at the time the offences were committed. She was convicted of one count of fraud by abuse of position and three counts of fraud by false representation under Sections 4 and 2 of the Fraud Act 2006 at an earlier hearing.

Her husband, Gary Poole, 67, was found not guilty of one charge of acquisition, use and possession, contrary to section 329(1) of the Proceeds of Crime Act 2002.

As well as overseeing the school's finances, Debra also oversaw the documentation used for any changes to staff pay.

She was also in charge of managing the invoices and finances for Woody's, the school's breakfast and after school club.

The court heard how Debra abused her position as signatory of the club's bank account between 14 October 2011 and 10 October 2018 by transferring funds, writing out cheques to herself and then cashing the cheques. This amounted to a total of over £490K over the seven-year period.

Detective Constable Lloyd Ives, who investigated the case, said: "I hope that the sentence given to her today shows the seriousness with which such a massive abuse of trust and position is taken and I hope that it is a deterrent to anyone else thinking of committing similar offences that it is simply not worth the risk – you will get found out."