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

Black Friday deals – shop safely over the festive period

Online shopping provides criminals with an opportunity to deceive people on shopping and auction sites and via social media selling platforms. This could be by paying for goods and services that don't exist, or through using images taken from genuine sellers to convince you of the legitimacy of a product. Be aware of fake brands and counterfeit goods.

Criminals will sometimes use cloned websites to convince you that you're purchasing from a genuine site. They may also ask for upfront payments, or send you fake receipts and invoices that appear to be from the payment provider.

This time of year we see buyers paying deposits for electronic goods, in particular games consoles, mobile phones and other electronic devices and subsequently never receiving the products. You may also be asked for payment for courier delivery services or insurance when buying and selling online.

Top Tips

- Stay on the website – be wary of being asked to move to a different platform
- Use the recommended payment method or you may not be eligible for a refund
- Do some research – check the sellers history
- Check the URL of the website – it may have been cloned
- Do not pay by bank transfer
- Fraudsters may offer items for sale at a discounted price, the deals may sound too good to be true
- Sellers may pressure you into making a quick decision due to it being a limited offer or similar

Financial abuse by a known person

Financial Abuse comes in a number of guises. Sadly we have seen cases increase across Sussex and Surrey with 34 cases recorded just last month with a financial loss to victims totalling £8,332.62.

The cases span a variety of MOs but include:

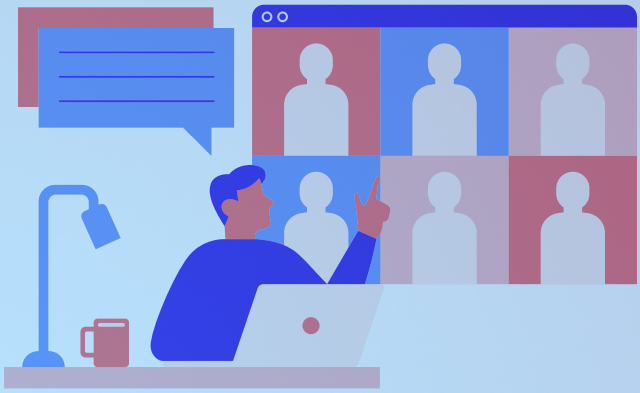
- **High instances of abuse by carers. Victims have trusted them to help with their shopping and given them their bank card and pin, and the carer then takes advantage of this and starts using the victims card for their own benefit.**
- **We have also seen similar examples where grandchildren are being trusted to help care for their grandparents and go on to abuse their trust by using their bank card for their own gain, or stealing blank cheques and filling them in.**
- **Another target are those with mental health concerns – people known to them have been using and financially exploiting them for their own gain, including attending the banks with them, asking them to withdraw money and hand it to them, on some occasions to purchase illegal drugs.**

Did you see our free Cyber Security Webinar last month?

"Cyber Security For Humans – Easy tips to stay safe in a digital world" were a series of accessible webinars we ran to give you all the information you need to massively reduce your chance of becoming a victim of cyber crime and online fraud.

Don't worry if you missed the live session, a recorded version can be found here on YouTube:
Cyber Security Advice From an Expert - Easy Tips to Stay Safe in a Digital World - YouTube

Please be sure to complete the one minute survey to let us know if you want more events like this:
General awareness (individuals) engagement survey 23/24 (smartsurvey.co.uk)



Phishing - do you know how to spot malicious emails?

- Ask yourself, were you expecting this communication?
- Is the message trying to make you panic or promote a sense of urgency or scarcity to entice you to click a link?
- Often phishing messages will be written in poor english and contain grammar and spelling errors.
- In the workplace, phishing emails are often sent on a Friday before people leave for the weekend.

What can you do?

- Check the senders address and the link text. Hover over it with your cursor and you will usually see red flags. Instead of www.nhs.uk you may see a subtle variation such as www.nh5.ru or www.nhs.uk-403431.uk
- Don't click links. Close the message and go to the relevant website to get to where you need to go.
- Is your friend or family member sending you something that doesn't seem right? Or claiming to be contacting you after losing their phone? Be suspicious. Contact them via a trusted and usual method (or third party) and ask if they sent the message to you. They will likely tell you their account was hacked recently so don't click on anything sent.
- Another tip – if you are using a modern email provider such as Gmail or Outlook, you can mark malicious emails as spam and report to report@phishing.gov.uk. Your email provider will learn from what you're marking as spam and filter out more of these emails so you get less of them in the future.