REPORTING A CYBERCRIME

We all make mistakes and these days the scams can be incredibly convincing.

If you think you, or someone you know has been a victim of online fraud let your bank know what's happened immediately.

Report the offence to **Action Fraud**
0300 123 2040
or via their website
www.actionfraud.police.uk

The new **COVID Fraud Hotline**
0800 587 5030
has also been set up by in partnership with CrimeStoppers to enable individuals to report fraud within the public sector during the pandemic. There is also an online reporting feature which can be found here: http://covidfraudhotline.org

If you need to seek further advice you can contact us via one of the following methods:

- Facebook: send a private message to DerbyshireConstabulary
- Twitter: direct message our contact centre on @DerPolContact
- Complete the online contact form www.derbyshire.police.uk/contact-Us
- Call us on **101**.

Please share this warning with friends and family so we can prevent anyone from falling victim.

USEFUL RESOURCES

DIGITAL MOT
Complete a digital MOT a useful tool to help you be more secure online:
www.saferderbyshire.gov.uk/what-we-do/cyber-crime

RURAL ACTION DERBYSHIRE
We have trained "Cyber Buddy" volunteers to help people across Derbyshire who would benefit from one-to-one digital support, for those that struggle with using the internet.

Email: j.dugdale@ruralactionderbyshire.org.uk
or call and leave a message on **01629 592970**.

LITTLE GUIDE to
PREVENTING FRAUD and CYBER CRIME
Visit the Metropolitan Police's 'Little Guide to Preventing Fraud and Cyber Crime' for a series of books and videos on how to avoid falling victim to a scam at: www.met.police.uk/littlemedia

For further information or advice, please contact Derbyshire's Fraud & Protect Officer Tammy Barnes via email: Tammy.Barnes@Derbyshire.Police.uk

101 in an emergency always call 999
www.derbyshire.police.uk

@DerbysPolice | Find us on | Follow us on

DC vulnerableelderlyscams 0221

KEEP ALERT
BE FRAUD AWARE

Fraudsters are currently targeting the vulnerable and elderly in your area.

We want you to be fraud aware, be on the lookout for the following offences and scams currently in circulation

Making Derbyshire Safer **Together**

Courier and Banking Fraud

Courier fraud occurs when a fraudster contacts a victim by telephone, purporting to be a police officer. Lately, we have seen an increase in calls across Derbyshire leading to many loosing thousands of pounds to this scam.

The caller might be able to confirm some easily obtainable basic personal details, such as your full name and address, to convince you this is an official call.

The scam

Scammers may state they are calling from the Serious Fraud Investigations Unit or that they are an officer from various forces - going by names such as PC/DC Clarke.

After some trust has been established, the fraudster will then, for example, suggest:

- Some money has been removed from a victim's bank account and staff at their local bank branch are responsible.
- Suspects have already been arrested but the "police" need money for evidence.
- A business such as a jewellers or currency exchange is operating fraudulently and they require assistance to help secure evidence.

Victims are then asked to co-operate in an investigation by attending their bank and withdrawing money, foreign currency from an exchange or purchasing expensive items, such as gold bullion or rolex watches to hand over to a courier for examination who will also be a fraudster.

How to protect yourself

- If you receive such a call you should not give out any personal information and hang up the call immediately.
- The police will never contact you asking for banking information, request that you withdraw money from an account or ask for you to purchase jewellery/gold to aid an investigation.
- If you need to call your bank to check if the call is official, wait five minutes after the initial scam call; fraudsters may stay on the line after you hang up. Alternatively, use a different line altogether to call your bank.

Romance Fraud

Romance fraud offences occur when an individual believes that they've met their perfect partner online, but the other party involved is using a fake profile to form a relationship and over a course of weeks or months, gains the trust of the individual - with the criminal's end goal being to steal money or personal information from their victim.

No matter how long you've been speaking online and how much you trust them, if you haven't met them in person

DO NOT:

- Send them any money.
- Allow them access to your bank account.
- Transfer money on their behalf.
- Take a loan out for them.
- Provide copies of your personal documents (e.g. passport).
- Invest your own money on their behalf or on their advice.
- Purchase and send the codes on gift cards from Amazon/iTunes.
- Agree to receive and/or send parcels on their behalf (e.g. laptop).
- Purchase high value goods, such as mobile phones or contracts.

Identity theft in the online dating world is also a growing trend and many people have fallen victim to having their personal data used without their knowledge or consent - some people might know this crime as 'catfishing'.

How to protect yourself

- Exclude important personal information from your profiles.
- Don't rely on default social media privacy settings.
- Create strong and unique passwords.
- Watch out for 'phishing' emails.
- Keep your browser and antivirus software up-to-date.
- Block any users that arouse suspicion.
- Regular check your mailbox to look for suspicious activity.

Ensure that your social media connections are who they say they are - when in doubt, throw them out.

Email and Text Phishing Scams

A number of phishing emails and texts have been circulating, in particular, surrounding Covid scams. These messages contain links and attachments that send individuals through to fake websites, attempting to coerce people into divulging personal or financial information.

In particular, look out for messages claiming to be from the UK Government, HRMC, NHS Test and Trace or NHS vaccine emails. If you receive a text or email that asks you to click on a link or for you to provide information such as your name, credit card or bank details, it's a scam.

Any text message containing a link should be treated with caution. The best way to find information from GOV.UK, or any other agency, is to visit that particular website via a trusted source and do not click on links in unsolicited texts or emails.

How to protect yourself

Scams can come in many forms and is an incredibly sophisticated crime, making it more difficult to distinguish genuine messages from the fake.

- Do not open attachments or click on links in emails or texts from senders you don't know.
- Never give out personal information, financial details or passwords in response to an email, text or phone call without verifying that the person is who they claim to be.
- Block any numbers that arouse suspicion.
- Set up spam filters on all of your accounts.
- Always go to a website directly, by typing out the address yourself, when logging into an account.
- Look out for fake websites by sense-checking the domain name.
- Keep an eye out for numerous spelling mistakes in messages, these are normally linked to phishing emails and texts.

Cold calls regarding the vaccine are also beginning to take place, where scammers are asking people to pay for the vaccine over the phone. If you receive one of these calls, hang up.