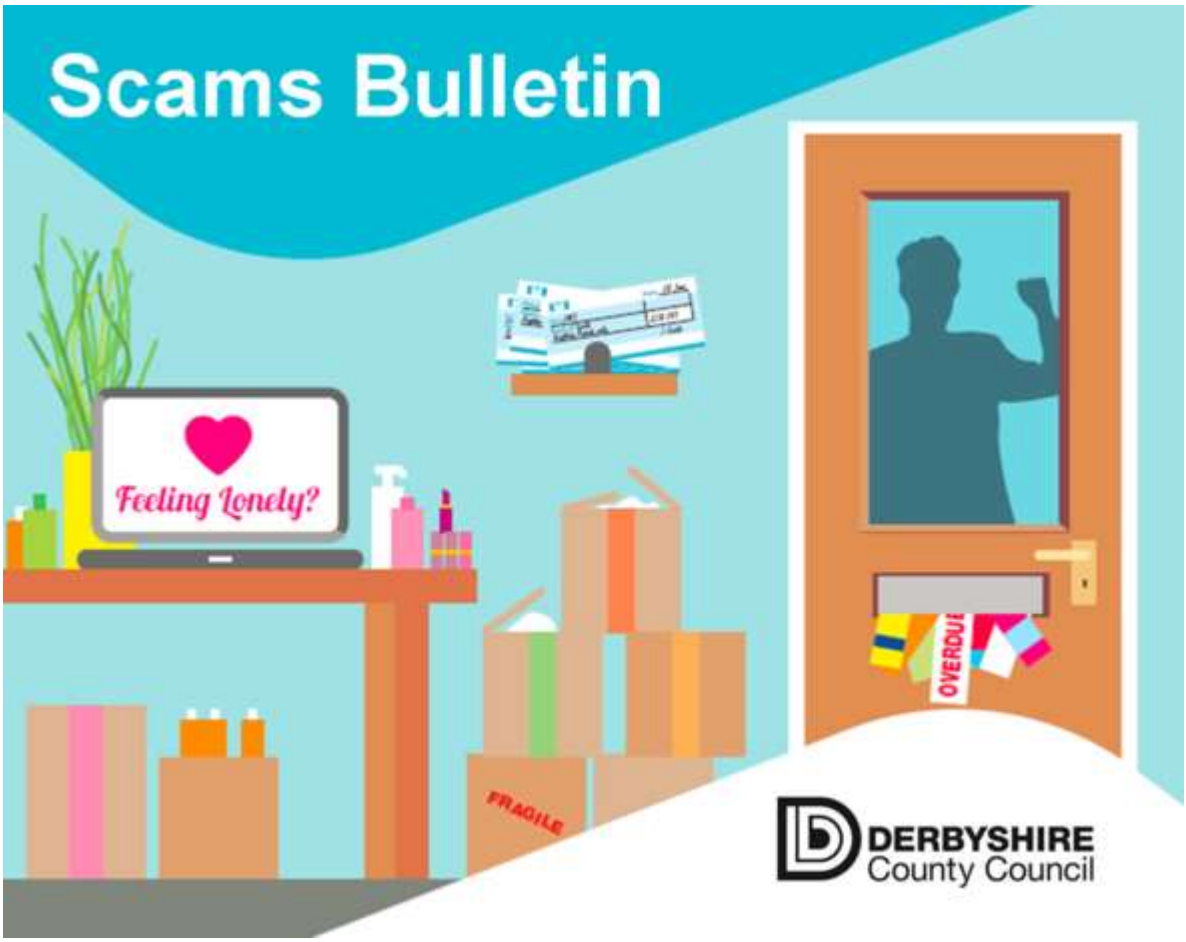

Welcome to the Sixth Edition of the Derbyshire County Council Scams Awareness Bulletin

February 2018 - Edition 6

This bulletin gives details of scams that council staff have been made aware of in recent weeks. Please feel free to share this bulletin far and wide - you can send it to colleagues, family members or friends as it is a public bulletin.

Police issue warning about romance fraud

With Valentine's Day just gone, love may still be lingering in the air but Derbyshire Police are warning residents not to be taken in by online scam artists.

Criminals are using social media to con people into handing over thousands of pounds – with one Derbyshire victim recently duped out of more than £110,000.

Vulnerable victims are being manipulated into sending cash to people they believe are genuine love interests but are in fact criminals.

Conmen are using social media to target individuals looking for love and companionship and after building what appears to be a loving relationship, the fraudster will create a crisis situation and ask the victim for money to help them.

Find out more, including top tips on how to protect yourself on the Derbyshire Constabulary website.

Phantom debt fraud

Action Fraud reports that there has recently been an increase in the number of calls to members of the public by fraudsters requesting payments for a “phantom” debt. The fraud involves being cold-called by someone claiming to be a debt collector, bailiff or other type of enforcement agent. The fraudster may claim to be working under instruction of a court, business or other body and suggest they are recovering funds for a non-existent debt.

The fraudsters are requesting payment, sometimes by bank transfer and if refused, they threaten to visit homes or workplaces in order to recover the supposed debt that is owed. In some cases, the victim is also threatened with arrest. From the reports Action Fraud has received, this type of fraud is presently occurring throughout the UK.

It is important to recognise that there are key differences between the various entities who seek to settle debts or outstanding fees in England and Wales. These differences range from the type of debt they will enforce to the legal powers they possess. To learn more, please take a look at some of the helpful information and links on the Step Change Debt Charity website.

Protect Yourself

- Make vigorous checks if you ever get a cold call associated with a bailiff.
- If you work for a business and receive a call or visit from bailiffs or debt collectors, be sure to speak with your manager or business owner first. Never pay the debts yourself on behalf of the business you work for; some fraudsters have suggested employees do this whilst talking with them, suggesting they can then be reimbursed by their employer, when in reality the debt is non-existent.
- Request details of the debt in writing to confirm its legitimacy.
- Do not feel rushed or intimidated to make a decision based on a phone call. Take five and listen to your instincts.

You can report suspicious calls like these to Action Fraud by visiting www.actionfraud.police.uk or by calling 0300 123 2040.

Flight ticket fraud

Fraudsters are attempting to entice victims who are looking for cheap flights abroad. Victims have reported booking tickets via websites or a “popular” ticket broker, only to discover that after payment via bank transfer or electronic wire transfer, the tickets/booking references received are counterfeit.

Fraudsters are targeting people who are seeking to travel to African nations and the Middle East, particularly those wishing to travel in time for popular public and religious holidays.

Prevention Advice:

- Pay safe: Be cautious if you're asked to pay directly into a private individual’s bank account. Paying by direct bank transfer is like paying by cash – the money is very difficult to trace and is not refundable. Wherever possible, pay by credit card or a debit card.
- Conduct research on any company you’re considering purchasing tickets from; for example, are there any negative reviews or forum posts by previous customers online? Don’t just rely on one review - do a thorough online search to check the company’s credentials.
- Check any company website thoroughly; does it look professional? Are there any spelling mistakes or irregularities? There should be a valid landline phone number and a full postal address so that the company can be contacted. Avoid using the site if there is only a PO Box address and mobile phone number, as it could be difficult to get in touch after you buy tickets. PO Box addresses and mobile phone numbers are easy to change and difficult to trace.
- Be aware that purchasing tickets from a third party, particularly when initial contact has been made via a social media platform can be incredibly risky.
- If tickets to your intended destination appear cheaper than any other vendor, always consider this; if it looks too good to be true, it probably is!
- Look for the logo: Check whether the company is a member of a recognised trade body such as ABTA or ATOL. You can verify membership of ABTA online, at www.abta.com.
- If you have been affected by this, or any other type of fraud, report it to Action Fraud by calling 0300 123 2040, or visiting www.actionfraud.police.uk.

Fake vouchers scams

Sainsbury's Vouchers

Fraudsters are sending out fake Sainsburys gift vouchers via email.

The email claims that the intended victim was overcharged on a recent visit to the supermarket and offers the gift card as compensation. However, when users click the link to get to the promised gift vouchers, they are led to a website that could potentially defraud them

ITunes Vouchers

Gift cards being used as part of HMRC scam that sees bogus debts and taxes paid using iTunes gift cards.

Fraudsters duped one victim into handing over £15,000 worth of gift cards. Officers are issuing this advice as the tax deadline has passed and penalties are being issued.

Detective Inspector Debbie King, who leads Derbyshire police’s economic crime unit, said: “Criminals are always changing the methods they use and this is the latest ruse to defraud people of their money.

“This type of crime is often directed at vulnerable members of society who are more likely to be taken in by this type of fraud.

“iTunes gift cards are easily redeemed and easily sold on. Scammers don’t need the physical card to redeem the value and instead get victims to read out the serial code on the back over the phone.

“The same scam has been used in the USA where criminals posed as attorneys, debt collectors and even police officers.

“We have been backing the Take Five campaign and I would urge anyone to take five minutes to make sure they pass the below advice onto friends, family and colleagues.”

Security schemes such as the Banking Protocol are designed to stop people from withdrawing large amounts of money unchallenged, however, this scam bypasses those procedures and can leave people thousands of pounds out of pocket.

Fraudsters are contacting victims in three ways: voicemails, spoofed calls or text messages.

Find out more about this scam including how to protect yourself on the Action Fraud website.

Improve your internet security in two minutes - for free

Domain Name Systems (DNS) are like public phone books for the web. They’re the reason you only need to remember a website’s name and not its IP address (think of these as phone numbers for computers). When you type “www.youtube.com” into a browser, a DNS service translates that into the associated IP address (199.223.232.0) for you.

Imagine a phone book that automatically filters and removes phone numbers known to be used for fraud. That’s what Quad9 does for websites. Quad9 provides an automated way to protect yourself and your business by blocking access to known malicious websites, like phishing sites designed to steal personal or banking details.

Quad9 checks the website to determine if it’s malicious.

Visit https://quad9.net for a step-by-step guide on how to improve your online security in two minutes.

Scams you've told us about

In previous editions of the Scams Bulletin we asked you to send in details of any scams you've experienced recently. Here's what you told us:

Email scams

Example 1: I recently received a message saying I was due a refund of some overpaid road tax. The site appeared genuine, but went on to ask for bank details so they could send the refund to me. Needless to say I did not reply, and reported it to DVLA

Example 2: My mother has received an email addressed to my father relating to an order of a Virgin experience day which he knows nothing about. It had the correct home address, father's first name (but no surname stated) and mobile number. The email reads as follows

Hi xxxxx, Your order has been received successfully. Your order reference is DH 998 0937. FX. (This is a link in blue.) Best regards The Virgin Experience Days Team

You can check details and status of your order by clicking on this link. (Which of course we have not)

The order is for an introductory helicopter lesson costing in total 202.99.

Most suspicious and alarming for my parents as they are pensioners. Please spread the word.

Example 3: I received an email claiming to be from HMRC stating 'This is an official email received from HM Revenue & Customs'. The email told me I 'still' hadn't claimed a tax refund of £260.19 and if I wanted to claim it, all I had to do was click on a link and complete a form. I obviously didn't click on the link but it was clearly a scam because the actual email address was an @org.au email address.

Telephone scams

Example 1. After reading your latest scam bulletin I thought I would share the following: I received three automated phone calls on my landline (which is registered with TPS) claiming to be from the HMRC asking "me or my solicitor to call back immediately regarding a time sensitive issue, our hotline is 02031296762. Call or legal action will be taken, goodbye and take care"

The three automated messages were all slightly different but followed the basic set pattern above and gave the same number to call back. The calls were from London numbers.

I didn't call back or give them any information. I forwarded the email to HMRC (using phishing@hmrc.gsi.gov.uk) who replied and confirmed it was a scam.

Example 2: I've had several phone calls stating I had overpaid monies to Sky. I told them to send it through the post. Nothing yet but I phoned Sky who knew nothing about it.

Example 3: I received a call from someone who greeted me by name and said she was phoning me on behalf of the UK Government to inform me of changes in banking legislation. She said that there have been bank charges made to my account over the years that are now to be refunded to me. She quoted my address and post code correctly, which I confirmed as that is 'public domain'. She then started with questions, first asking for my date of birth for security purposes… I decided that was the time to ask to receive the forms by post and hang up. I am not holding my breath.

Example 4: An elderly neighbour of mine recently got quite far down the road towards sending a £500 'Registration Fee' to receive the £10,000,000 she had 'won' in a competition she had not entered. Luckily she got suspicious just in time.

Example 5: I have today received a call claiming to be from HMRC telling me they are filing a lawsuit against me - press 1 to speak to my case officer. I did not do so. I have researched the number that dialled me - a Manchester area number - and it is indeed a scam.

Have you heard about a phone, postal, email or doorstep scam that's been happening locally? Or maybe you've come across an online scam or a copycat website.

Let us know so we can share the scam in the next Scam Bulletin to warn others.

Email adultcare.info@derbyshire.gov.uk

This bulletin will be sent out periodically based on demand. We can't guarantee to publish all the information you send in, but we'll try and make sure to get the message across.

Other national and local scam news

Rogue Traders

Police have warned the elderly to be alert to the dangers of rogue traders after reports after various people around the country have been targeted.

- One pensioner was approached by men who offered to carry out work on the roof of his property in Kent but quoted a very expensive prices.

- Three suspected rogue traders have been arrested in York after an elderly and vulnerable resident reported she'd been pressured into purchasing a new front door.

If you're in Derbyshire, avoid rogue traders by using the Trusted Trader register to find a reputable business.

Other scams

DBS Scam - A man who ran a large Disclosure and Barring Service (DBS) check fraud has been sentenced to five years and ten months in prison. The accused pleaded guilty to charges relating to websites he set up to process and charge for DBS checks for job seekers who had been told that they had been successful in their job applications. The jobs were fake and designed to trick people into paying for a fake DBS check. more

Fake Government Grants - Individuals and businesses are being warned to watch out for cold calls and online contact from fraudsters who are offering the opportunity to apply for Government grants for an advance fee. more

Facebook bans crypto currency adverts - the ban comes after a wave of complaints about the number of bitcoin or crypto-currency scams being promoted through the social network. more

Fake Argos texts - Criminals are sending a series of fake text messages to customers posing as Argos. They tell customers they are due a £180 refund for their "Argos card" and all they need to do to access the money is click on a link which subsequently asks for their bank details. more

Stop Loan Sharks Newsletter - you can read the Winter edition of the newsletter here.

Reporting scams and getting advice

Get advice from Citizens Advice Consumer Service, tel: 03454 04 05 06 or visit: www.adviceguide.org.uk

Report scams and suspected scams to Action Fraud or tel: 0300 123 2040.

Send potential **postal scams** with a covering letter to Royal Mail at FREEPOST Scam Mail, email: scam.mail@royalmail.com or tel: 03456 113 413.

Report unsolicited **marketing calls** to the Information Commissioner's Office or tel: 0303 123 1113.

Register phone numbers with the Telephone Preference Service or tel: 0845 070 0707.

The Mailing Preference Service (MPS) is free and can help reduce **unsolicited mail** by calling 0845 703 4599.

Contact the **Age UK Derby and Derbyshire** Information and Advice Line on tel: 01773 768240. Age UK also have a downloadable guide on recognising and dealing with all kinds of scams.

Derbyshire Scamwatch is a project funded by the Police and Crime Commissioner for Derbyshire. The aim is to raise awareness, particularly amongst older residents, of the potential harmful effects of mass-marketing, internet, doorstep and telephone scams and to provide one to one advice and support where potential scam/fraud victims are identified.

Tell a trusted friend, relative or neighbour.

Support for victims of scams

Age UK Derby and Derbyshire can provide help and support for older people and their carers if they've been affected by a scam or rogue trader. Local residents can call the helpline on tel: 01773 768240. Age UK also have regular information roadshows at events around the county.

Think Jessica is a Derbyshire-based charity set up to help and support people affected by scammers and also to highlight the effects on victims.

Derbyshire Victim Services offers free and confidential help to victims of crime and anyone else affected. Please tel: 0800 612 6505

The Derbyshire Trusted Befriending Network aims to help isolated and vulnerable adults find befriending services. For more information email befriending@sdcvs.org.uk or tel: 01283 219761.

Want to receive future editions of the Scams Bulletin?

If you wish to receive future editions of this bulletin and Adult Care newsletters, you can sign up by managing your subscriptions or you can email us at adultcare.info@derbyshire.gov.uk

This bulletin is compiled by the Adult Care Information Team

email: adultcare.info@derbyshire.gov.uk tel: 01629 531310

Find out more about scams: www.derbyshire.gov.uk/scams

DERBYSHIRE County Council

STAY CONNECTED: