derbyshire SCAM WATCH

Scams and Scammers

and How to Avoid Them

People in Derbyshire are being scammed out of their hard-earned money

Read this to learn how YOU can avoid becoming one of them

Further information from
www.derbyshirescamwatch.org.uk

For help with scams telephone **01246 252341**
or email **scamwatch@nedcab.org.uk**

Follow **Derbyshire Scam Watch** and get useful tips:

twitter.com/DerbysScamWatch

facebook.com/DerbyshireSW

citizens advice

Derbyshire Police and Crime Commissioner
Protecting Communities, Fighting Crime

IF IT LOOKS TOO GOOD TO BE TRUE IT PROBABLY IS!

United Kingdom authorities have estimated that at least £10 billion was lost to scams in 2017 affecting 3.2 million UK people

Who are targeted by scammers?

Everybody is a potential target and we are all likely to fall for some type of scam at some time in our life.

Unfortunately, some people are more vulnerable than others, particularly the elderly, lonely, and those who might struggle to make decisions. Others include people who may be ill or in debt and desperately seeking a solution to their problems.

However, be aware that **anybody** can be conned in the right circumstances, for instance when they are extremely busy or distracted by other things.

How do scammers work?

Scammers can approach you in many ways: by post, phone call, text message, email, website, social media and even in person on your doorstep or in the street; in fact in every way that people communicate.

They will quickly try to establish where your vulnerabilities lie and then exploit them. Scammers will often start by trying to get a small amount of money and then over time will increase the amount and introduce more scams to help themselves to your money.

Once a scammer is successful with a person they will sell on their details to other scammers (this is known as a "suckers list") and the scam attacks can then escalate very rapidly.

Scammers work on human nature to exploit desire or even greed. They encourage people to make decisions quickly to rush them into not thinking it through, and to keep it secret from their friends and family in case they are talked out of it.

Scams can look personal or official, and sometimes they are even threatening.

Scams fund organised crime and terrorism

The alleged winnings from postal scam mail received by one person over a six month period totalled £2.8 million – of course they received nothing at all

Common Postal Scams

Lotteries and Prize Draw Letters

You may get a letter to say that you have won a large sum of money in a lottery or prize draw and be asked to pay a fee or charge before you can collect it.

You might not remember entering the competition; that's because you never did and this a scam.

You might also be asked for further payments or to call a premium rate number before the prize is released.

The amount of money will be very tempting but you will never receive it.

A genuine lottery or prize draw will not ask you to pay a fee to collect your winnings.

You also might be asked for your bank details so that they can pay 'your winnings' directly into your account – don't, because they will use the information to clear out your account.

Other Types of Scam Letter

There are many other possible types of scam sent by post including:

- Inheritance letters
- Clairvoyant offers
- Catalogues
- Pyramid get-rich quick schemes

They all offer something that is intended to part you from your money and they can look very official – they are not. Letters will usually look as if they really come from an important source but with modern technology they can be easily made in just a few minutes on a computer. They will often show things like official looking stamps and photographs of their directors and will always try to rush you by giving bogus deadlines for reply.

The best way to deal with them is to destroy the letters. Do not try to contact the sender; if they do not get a response, they will eventually stop sending them.

Mail Preference Service (MPS)

You can cut down on excessive legitimate mail by registering with MPS online at **www.mpsonline.org.uk** or by telephone on **0207 291 3310**

By cutting down, you will be able to spot the criminal scam mail much easier.

Most scams in these pages can be made by any means, by post, telephone or online – so BEWARE…

Telephone – including mobile

Spam texts and calls will often offer services to claim against an accident, reclaim PPI, cash in a pension or get help with debts.

At best these services will cost you a large share of any legitimate claim but at worst they will cost you your savings and future financial stability.

Never respond to a spam text and always delete it.

Remember, you do not have to get into a discussion over the phone with anyone.

Keep your business your business. Just say "no thank you, I'm not interested" and then hang up.

Never give out personal information, especially bank or credit card details, by phone, text, social media or email.

Computer Problems?

Nobody will know if you are having problems with your computer, unless you tell them. If somebody rings you out of the blue to talk about "computer problems", just hang up.

Unsolicited calls from computer help services are always scams.

They want access to your computer so that they can cause damage and get your personal information. They will probably make your computer unusable until you pay them lots of money in ransom.

They will also leave spyware behind that can steal your confidential information, such as passwords, payment details and bank log-in information.

Telephone Preference Service (TPS)

You can cut down on excessive legitimate calls by registering with the Telephone Preference Service online at **www.tpsonline.org.uk** or by telephone on **0345 070 0707**

By cutting down, you will be able to spot the criminal scam calls much quicker.

There are some scams that would have you pay for TPS. Use these contact details and the service is totally free. It works for mobile numbers too.

Some people think that a web address starting with 'https://' is automatically safe but this only means that the communication to the site cannot be eavesdropped

Online Security

People now use their personal computers, tablets, mobile phones and other online devices for almost everything and there is an awful lot of personal information stored on them.

Yet most people do not protect the device or their online accounts with strong passwords and in some cases have no protection at all.

Protection does not have to be expensive, and certainly not as costly as being scammed.

- Protect all devices with strong passwords, use a mixture of letters (both upper and lower case) and numbers.
- Keep your computer and mobile devices all up to date
- Use a good quality antivirus app with firewall and anti-spam protection built in
- Use different passwords for each account – consider using a password vault to keep track of them

Typical Online Scams

Phishing is a way of stealing your personal information by email or web browsing.

It may be an email pretending to be from your bank asking you to 'confirm' your account details – no bank will ever do that – it is a scam.

An email might direct you to a website, it might be a rogue site that will steal your details. The website address shown in the email might not be the one it directs you to when you click it.

If you're not sure about an email you receive, don't click any links on it at all.

Email Attachments can let loose very damaging apps onto your device to steal your details or hold your device to ransom. Do not open any from an unknown sender.

If you get an email from a friend that looks strange and with an attachment, check with the friend (but not by email) to see if they sent it – their device might already be running a virus that has hijacked their device and sent the email.

Scam email. Never reply to this – to do so will confirm that the email reached you – you will then get more.

Do not let a burglar get in your back door whilst his accomplice keeps you talking at the front

Rogue Traders

Rogue traders can contact you online, by telephone, in the post or on your doorstep. They all have one thing in common: to part you from your money. If they actually get around to doing the job it may be overpriced and poor quality.

Rogue traders might use pressure selling and phony customer feedback to persuade you to buy their goods or services.

- Always check their credentials
- Get written quotes for the work
- View their previous similar work in your area if possible
- Use tradesmen recommended by people you know and trust
- Use tradesmen on registers like **Derbyshire Trusted Trader** or their trade body but don't rely on the trader's word, check the registering body yourself
- Get more than one quote for the job but remember that the cheapest is not always the best

Other Callers

Distraction burglary is where a caller to your front door keeps you talking whilst his accomplice enters your house through the back door and steals your possessions.

Always keep your doors locked.

Other callers may claim to be from many different organisations including local authorities, energy providers or charities. Always ask to see their ID and if you did not expect their visit check their credentials with their office. Don't just use the telephone number on their ID badge, it might be bogus, find the number from another source like a telephone directory or utility bill.

If you are still unsure then ask them to come back when you are not alone – a real caller will be happy to do that.

Derbyshire Trusted Trader online at www.derbyshire.gov.uk/community/trusted_trader or telephone on 01629 533190

The photo below shows the amount of "medicinal products" bought from mail-order catalogues by just one Derbyshire resident who thought they were in with a chance of winning a cash prize.

Helping Friends and Relatives

You may be able to help others by keeping your eyes open for signs that they have been scammed.

Typical indicators include

- Lots of recent purchases such as cosmetic samples or small trinkets
- Piles of letters, often in glossy envelopes designed to lure people in
- Financial hardship, like no heating in cold weather, empty food cupboards or piles of bills or final demands
- Self-neglect
- Isolation and a reluctance to talk about the scams
- Referring to the scammers as friends – they are sometimes the only regular contact the person gets

It is often difficult to help people who have been scammed for a long time because they are likely to be in denial but **Derbyshire Scam Watch**, in conjunction with **Derbyshire Trading Standards**, can help.

We can talk to people in their own homes to help them understand the problems and offer strategies to avoid future scams. We also work closely with **Citizens Advice** across Derbyshire to offer assistance with a whole range of problems, including debt.

Other Help

Derbyshire Scam Watch also works closely with other agencies across Derbyshire including **Derbyshire Police** and can refer people for assistance where appropriate.

Derbyshire Scam Watch is just a phone call away on 01246 252341
or email scamwatch@nedcab.org.uk

Criminals can easily find your details, including your name, so don't be misled into thinking they know you

Keep Safe

Do not answer unexpected email or letters unless you know who they are from and certainly do not give out personal information.

Simply answering these can give the criminal valuable information – just delete or bin them.

Do not give out personal information on the phone to unexpected callers – politely hang up.

Be extremely cautious who you give your details to when buying online.

Never send money or give card or bank details to somebody offering prizes, an inheritance or for the delivery of an unexpected parcel.

Keep your doors locked and always check the identity of callers. If a caller is not expected, check with their office to see if they have sent somebody but do not use the telephone number the caller gives you, find the number from somewhere else like letters and bills from the company.

Refuse entry if there is ANY doubt – a legitimate caller will not be upset by this.

Do not buy on the doorstep; you do not know who you are dealing with.

Computers, Tablets and Smart-phones

Allow updates to your devices – they are often for your own safety.

Protect them and your information with quality Internet security products – they must at least offer firewall, antivirus and anti-spam.

Protect mobile devices with password access but do not use the ones that criminals can guess easily.

These are suggestions on how to stay safe but it is not a comprehensive list

All personal advice is given in strictest confidence.

Remember...

IF IT LOOKS TOO GOOD TO BE TRUE IT PROBABLY IS!