Your essential guide to help prevent **FRAUD**

Stop. Think. Tell.

Making Derbyshire Safer **Together**

DERBYSHIRE CONSTABULARY

This is Claude, our fraud puppet. Whilst this might not be the most conventional way to get fraud prevention advice out there, we wanted to try something different.

This is in the hope that next time you get a dodgy call, email or message, this bright pink puppet will pop up in your mind and remind you to **Stop.Think.Tell.**

Anyone can be the target of a scam – these criminals know that we're all often busy people so are only paying limited attention to that risky link or call.

Listen to Claude and if you're not sure:

- **Stop** before clicking a link, giving your information or following the instructions from the caller.
- **Think** about what they're asking for, and why they say they need it. Banking and personal information is very valuable so consider carefully before giving any details.
- **Tell** another person or organisation. If you're still not sure about this request, talk to someone you trust – if you're ever in doubt, try and verify what's being asked and look for further advice in this booklet or visit: **www.derbyshire.police.uk**

Full details of how to report a scam are at the end of this booklet.

You might spot Claude popping up on our social media channels with these important crime prevention messages.

#SockItToTheScammers

Remember: If you think it's a scam: **Stop.Think.Tell.**

Contents

3	What is fraud?
4	Spoofing
5	Identity fraud
7	Money mules
8	Computer software service fraud
9	Postal scams
11	Courier fraud
13	Doorstep fraud
15	Investment fraud
17	Romance fraud
20	Cost of living scams
22	Selling Site Scams
24	Delivery charges
25	WhatsApp friends and family crisis
26	Online shopping
28	Buying pets online
30	Scam protection
33	The role of action fraud
36	Contacts
38	Derbyshire Alert
39	Final reminder

Derbyshire Victim Services

Where can I get **help** if I have been a victim of crime?

Talk to **us** our service is free, confidential and we are here to help.

We can provide you with practical and emotional help in the following ways:

- Someone to talk to and listen to you
- Someone to help you access a wide range of specialist support agencies
- Someone to help you with a Criminal Injuries compensation claim
- Someone to assist with whatever you need to help you cope and recover from the crime

We work with a wide range of specialist support providers across the county and can provide any help you might need in accessing these services. Whatever level of help you need, that's what we are here to provide.

All support will be provided at your own pace and only ever with your consent.

Open: Monday - Friday 8am - 8pm Saturday 9am -1pm

0800 612 6505 Text: DVS to 82228

support@dvssupport.org

www.derbyshirevictimservices.co.uk

What is fraud?

> Fraud by false representation, section 2 of the fraud act.
>
> This involves the criminal scamming the victim by lying or misrepresenting the situation.
>
> The term scam is a slang term for personal fraud.
> Fraud can affect anyone, and we know it is vastly under reported which makes it difficult to estimate the actual cost to the public in the UK.

There are essentially four ways a fraudster approaches potential victims. We refer to these as four fraud enablers and they are:

- Telephone
- Doorstep
- Postal
- Online

Whilst there are many variations of the types of fraud committed using the four enablers, we have produced a booklet outlining the most common we see in Derbyshire with practical advice on how to spot the fraud, and what to do to prevent you from being a victim of that type of fraud.

Spoofing

> **Phone numbers and email addresses can be spoofed by criminals to appear as though they are from someone, or somewhere, other than the actual source.**

Email and telephone spoofing tools are widely available, and criminals often use them as part of phishing attacks. Because the spoof number or email address is cloned, any spoofed communication will drop into any pre-existing threads of email or text communications you have.

Stay safe

The simple advice is never assume someone is who they say they are.

- Be suspicious if someone tries to draw your attention to the email address or telephone number displayed to prove their identity.
- Be wary of emails requesting any changes to payment methods, and always ensure if paying by bank transfer the account details match the account holder details.

Identity fraud

> **Your details are valuable to criminals and can be used by them or sold to others.**
>
> **If your data is obtained, it may be used to obtain credit cards or bank accounts in your name, as well as numerous other financial products.**

Criminals can use stolen data to access your bank accounts savings, or pensions. Because they know these basic details, they will then contact you and convince you that they are calling from your bank or from law enforcement and con you into providing the missing information they need. Your details can be obtained in several ways, from letters or bank statements you throw away, or information stolen from your computer. If you become a victim of identity fraud, it may severely affect your credit rating and it can take a significant amount of time to rectify this.

Stay safe

- If you start to receive post from a company or organisation you don't know, contact them, and find out why it is being sent to you.
- Sign up to a reputable credit rating agency. You will receive notifications of any activity seeking review any checks conducted on you.
- Be wary of unsolicited phone calls, emails or text messages purporting to be from your bank or your phone provider especially they ask for passwords or your date of birth.

Identity fraud continued

- Review your bank and credit card statements for any suspicious activity.
- Ensure you dispose of your private documents completely, for example by shredding them or burning them.

If you have been a victim of ID fraud, CIFAS offers protective registration to people who have fallen victim to, or are at risk of ID fraud.

Visit: www.cifas.org.uk

Money mules

> **Where financial gain comes from crime, criminals use banking systems to move their proceeds (stolen money).**
>
> **The account used to launder the criminal funds becomes a 'mule account', making the account holder a 'money mule'. People are often targeted to provide access to their accounts either on the promise of a share of the fund or by coercion.**

Criminals are always looking for alternative ways to launder the proceeds of crime. Unfortunately, this now includes clever marketing where young and vulnerable people are targeted.

Fraudsters use social media and online forums to post adverts offering the opportunity to make 'easy money' 'free money' or fake jobs using terms like 'squares' 'AC' 'flips' 'easy cash schemes' 'no risk money' or 'money transfer jobs'. Direct recruitment is made through word of mouth from people they may loosely know or through saying they are from a known school, college, university, or sports club. They may even use celebrity endorsements!

So, if you allow your bank account to be used by an unauthorised person or have criminal funds go through the account, you become a 'mule'. There is a risk that your account will be closed, and you will be reported to credit agencies.

You could find yourself prosecuted under the proceeds of crime act and facing up to 14 years in prison!

Stay safe

Never give anyone details of your bank or any other financial account; your bank card, PIN code, password, or pass code - bank/financial accounts are private

Don't be lured or persuaded to receive money into your account, even as a one off no matter how plausible it sounds.

Be suspicious, question what you're being asked to do and do your research.

Computer software service fraud

> Criminals may cold call you claiming there are problems with your computer, and they can help you solve them.
>
> They often use the names of well-known companies such as Microsoft or Apple. They may use the name of your broadband provider to sound more legitimate or tell you they are acting on behalf of your service provider.

The criminals may ask you to complete several actions on your computer. They then usually instruct you to download what is known as a 'remote access tool'. This gives the criminal access to everything on your computer. They can then access and copy your data or download malware onto your computer to monitor what you do in the future.

Fraudsters can even access your online banking, and transfer money between your accounts.

You may also be asked to pay for the assistance you have been given. This could be a one-off payment or an ongoing direct debit over many months or even years. If you do provide payment details, these may be used to commit further fraud against you.

Stay safe

- Genuine computer companies don't call you out of the blue, neither will your broadband provider.
- Don't let anyone remotely access your computer.
- If you are having issues with your computer, contact the retailer you purchased it from regarding service and repair. If you are having issues with your Internet speed or service, contact your service provider for further advice or support.
- If you think you have been a victim of this type of fraud, you must have your computer checked by a reputable company who will be able to remove any remote access tools.

Postal scams

Many victims of scam mail, also known as mass marketing fraud, are drawn in by the thrill of a guaranteed win.

You will part with money to claim a prize that does not exist. Often, victims of this type of crime are elderly or vulnerable. They are targeted because they may live alone or have access to significant savings or pension funds.

There are numerous types of scam mail, some more obvious than others. Be wary of what you reply to, particularly if you are asked to send money or provide personal information.

The letters may claim you have won a prize draw; competition or lottery you have not even entered. The letters will be personally addressed to you, giving the illusion you have been specially selected. Your name may appear numerous times within the letter, using words like guaranteed winner.

They will request a fee to claim your prize. This fee may be advertised as a delivery cost or administration cost. Fraudsters may also try to obtain personal details such as bank account or date of birth.

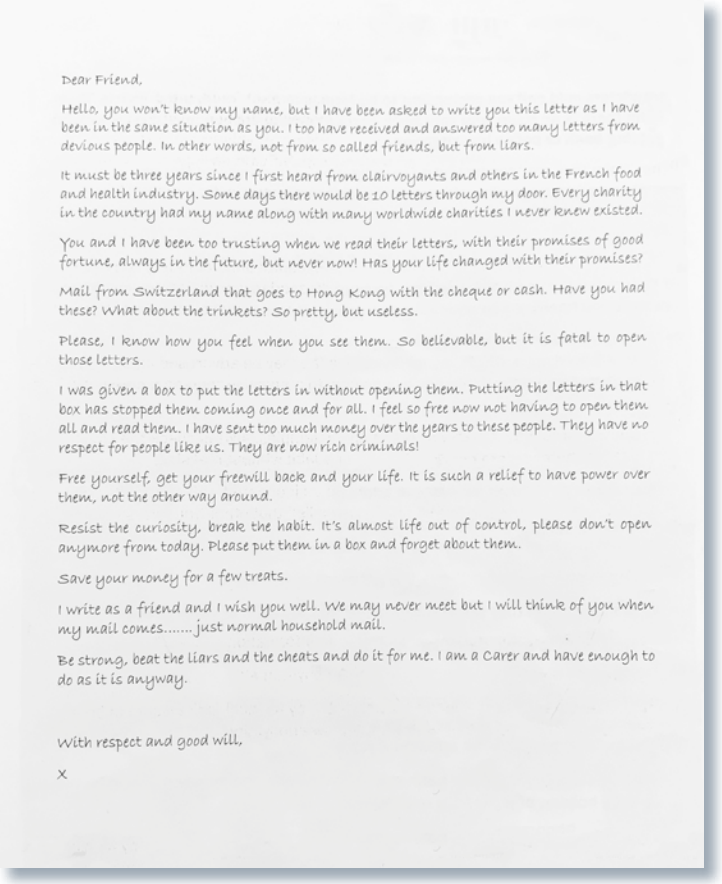
Be wary of letters offering discounted goods or samples. Always check the small print and make sure you are not agreeing to a direct debit without realising.

It only takes a single response to scam mail, to be inundated with more. After this response your details will be added to a victims list that other fraudsters will have access to.

If you receive a letter that doesn't seem right, think of Claude and **Stop.Think.Tell.** Take a moment before providing any details and read over the prevention advice.

Stay safe

- You cannot win a prize if you have not entered. Be wary of anyone asking you for private information, ask yourself why am I being asked to make payments?
- Please have a read of this letter below, it was written by a postal fraud victim to other fraud victims. It has been adapted for anonymity.



Dear Friend,

Hello, you won't know my name, but I have been asked to write you this letter as I have been in the same situation as you. I too have received and answered too many letters from devious people. In other words, not from so called friends, but from liars.

It must be three years since I first heard from clairvoyants and others in the French food and health industry. Some days there would be 10 letters through my door. Every charity in the country had my name along with many worldwide charities I never knew existed.

You and I have been too trusting when we read their letters, with their promises of good fortune, always in the future, but never now! Has your life changed with their promises?

Mail from Switzerland that goes to Hong Kong with the cheque or cash. Have you had these? What about the trinkets? So pretty, but useless.

Please, I know how you feel when you see them. So believable, but it is fatal to open those letters.

I was given a box to put the letters in without opening them. Putting the letters in that box has stopped them coming once and for all. I feel so free now not having to open them all and read them. I have sent too much money over the years to these people. They have no respect for people like us. They are now rich criminals!

Free yourself, get your freewill back and your life. It is such a relief to have power over them, not the other way around.

Resist the curiosity, break the habit. It's almost life out of control, please don't open anymore from today. Please put them in a box and forget about them.

Save your money for a few treats.

I write as a friend and I wish you well. We may never meet but I will think of you when my mail comes..... just normal household mail.

Be strong, beat the liars and the cheats and do it for me. I am a Carer and have enough to do as it is anyway.

With respect and good will,

X

Visit: **www.friendsagainstscams.org.uk/scammarshals**

Courier fraud

Fraudsters cold call you pretending to be from your bank or from the police.

They claim there is an issue with your bank account or request your assistance with an ongoing bank or police investigation.

They claim they are conducting an investigation, often saying it involves corrupt bank employees/corrupt police officers/ counterfeit money/counterfeit high-value goods. They ask for your help or say your account is at risk. The aim of this call is to trick you into parting with your money or the high-value goods you have been told to purchase either in person, online, via a money service bureau or in a bank.

If they manage to convince you, they instruct you to carry out a task which ultimately involves you handing over your money or goods.

These include:

- Asking you to attend your bank branch to withdraw a large sum of money which will then be collected from you as evidence. They may claim the money could be counterfeit, that it is going to be sent for forensic or fingerprint analysis.
- Asking you to withdraw large amounts of foreign currency, which will similarly be collected by a courier from your home address.
- Asking you to provide details over the phone, including your pin then handing over your cards to a courier sent to your address.
- Asking you to purchase high-value items such as expensive watches to clear criminal funds which will again be collected by courier.

Courier fraud continued

- Asking to purchase other items, like gift cards or vouchers. In all these cases they will assure you that you will be soon reimbursed.

Fraudsters want to avoid detection, and may give you instructions to achieve this such as:

- Informing you it is an undercover operation involving the bank/police corruption, so you must not tell bank staff or police anything about the phone call. They may even threaten that you could be arrested if you do.
- Give you a cover story to tell bank staff or police, example the money or item is for building works, a holiday, or a gift for a relative.

Stay safe

- Your bank or the police will never ask you for your PIN, bankcard, or ask you to withdraw money or buy items on their behalf.
- If you receive an unexpected call, hang up and use another phone to call back and confirm identity on a number you can verify yourself, not one given to you by the caller.
- Ask yourself how do I know they are who they say they are?

Doorstep fraud

Doorstep fraud involves criminals knocking on your door and unexpectedly offering products or services.

Fraudsters convince you to pay for goods or work which is often overpriced, or poor quality or is not even carried out. In many cases, this work isn't even necessary. They may use intimidation and pressure you to make quick decisions so that you agree to their demands.

Criminals may try to convince you that work is urgently required and the price they are charging is fair. They will put pressure on you to have the work done immediately and may ask for payment upfront. Often the work is not completed, or if it is, the work is to a poor standard. You may also be overcharge for any work done.

They can use deception to convince you by;

- Claiming they were working in a neighbour's address and noticed you needed work completing and they have the materials.
- Inspecting areas, you can't access, for example the loft or roof and show you photos or videos claiming they are evidence that you need the urgent repairs.
- Throwing water down when you are not looking to indicate you have damp.
- They may be insistent you pay in cash immediately or put down a deposit, even offering to take you to the bank to get the money. If you do not do this, they may continue to find reasons for you to pay more money.
- Some callers will be legitimate. If they are, then they will be more than happy to wait whilst you check them out using a number you can verify yourself, not one supplied by them.

Doorstep fraud continued

Stay safe

If you are not sure, then don't open your door. Callers can show you their official credentials through a window without you opening your door.

If you are not happy about someone's identity, do not let them into your house under any circumstances. You don't have to open the door to say "no thank you" to someone. Legitimate builders do not call door to door and they would never expect you to pay upfront for their services.

If you do let someone in, never leave your front door open unlocked or unattended, so a second individual can't enter without your knowledge.

Remember, **Stop.Think.Tell.** You should never agree to work straight away, just because someone is on your doorstep.

A legitimate trades-person should have no issue with you checking with a trusted friend or family member before making a decision."

Investment fraud

Investing in stocks and shares or any other commodity can be a successful way of making money.

However, it can also lead to people losing their entire life savings. Criminals will persuade you to invest in all kinds of products. They will offer you high rates of return, particularly over longer periods of time, which often don't exist.

Common products offered include binary options, virtual currency, carbon credits, wine, rare minerals, gemstones, land, and alternative energy. Often, initial investments will yield small returns as an incentive to invest further funds. However, larger investments or cashing out will be met with excuses or a penalty charge. Eventually contact with the fraudster will be impossible and all funds and bogus returns lost.

Fraudsters are organised and they may have details of previous investments you have made or shares you have purchased. Knowing this information does not mean they are genuine.

Criminals may direct you to well-presented websites or send you glossy marketing material. These resources do not prove they are a genuine company. Many fraudulent companies have a polished customer image to cover their illegal activities. It is relatively easy to register a company with Companies House. This does not confirm or endorse that they can provide genuine investment. Indeed, emerging investment markets may be unregulated, making these open to abuse.

Investment fraud continued

Companies may be registered at prestigious addresses. This does not mean that they operate from there. It is an accepted business practice to rent such a virtual office to enhance a business status. However, fraudsters are also aware of this and exploit it.

The fraudster may put pressure on you by offering a once-in-a-lifetime opportunity and will claim the deal must be done quickly to maximise profit.

In addition-be wary of companies that offer to "recover" any funds you have lost to any sort of investment fraud. They may be linked to the company who initially defrauded you in the first place and may be targeting you again. This is called recovery fraud.

Stay safe

- There's no such thing as a 'guaranteed risk free' investment. High returns can only be achieved with high risk.
- Don't be pressured into making a quick decision.
- Seek independent financial advice before committing to any investment.
- Ask yourself 'why would a legitimate investment company call me out of the blue?'

If you're not sure the company you are investing in is real, it could be a scam. Check the FCA register before investing.

Visit: www.fca.ord.uk/scamsmart

Romance fraud

> **Dating online is now one of the most popular ways for new couples to meet, with millions of people finding new relationships, romance and love this way.**
>
> **Unfortunately, amongst genuine profiles are fake profiles set up by fraudsters. They are often after your money, not your love. They are masters of manipulation, playing on your good nature and emotions to ultimately steal your money.**

Criminals will build a relationship with online members, quickly asking to move communications off the dating site. This is so they can continue their contact with you, even if their profile is later identified by the site as fraudulent and subsequently deleted.

Fraudsters are often very flattering, appearing really interested in you within a short space of time. However, they will use a range of excuses as to why they can't meet you in person, such as they are stuck overseas, have a family emergency, or have an issue with their business. They then start asking for money to help with their problems, assuring you will be paid back as soon as they can. The fraudster may claim to be desperate to meet you as soon as this obstacle is overcome. This is all a scam and their true intention is to take as much money from you as they can.

Stay safe

- Keep all communication on the dating website or app you are using.
- Don't be convinced by profile pictures, they may have been taken from somewhere else on the Internet.

Romance fraud continued

- Never send money to someone you have not met in person and be extremely wary of giving money to someone you have recently started a relationship with.
- Do your own research on the person-are they members of any social networking sites? Can you confirm what they are telling you about themselves, such as where they work or where they live?
- Be wary of anyone asking you to receive money on their behalf and transfer it on. They may be asking you to launder money.
- Talk to family and friends for advice, even if the other party is asking you to keep the relationship secret.

If you recognise the below pattern of behaviour and it feels familiar to you, you are not alone.

Please take some time to consider the questions, if you find yourself answering yes to some of them you may be a victim of a romance fraud

- ♥ Shortly after meeting they tell you they love you or have strong feelings for you. Yes ☐ No ☐
- ♥ They ask to communicate with you via personal email and away from the original site where you initially met. Yes ☐ No ☐
- ♥ They work in senior roles such as the CEO of a company or in another professional capacity such as a surgeon or dentist. Yes ☐ No ☐
- ♥ They work in remote locations such as an oil rig, war torn countries. Yes ☐ No ☐

- Their profile might not match what you read on the dating site, in which they feature, with everything they tell you. Yes ☐ No ☐
- As they gain your trust, they begin to tell you stories of bad luck or medical illnesses, even family tragedies. Yes ☐ No ☐
- They indirectly or directly ask for cash, gifts, or cash to pay credit cards. Yes ☐ No ☐
- Their messages might be poorly written, inconsistent and sometimes vague. Yes ☐ No ☐
- They offer various excuses for why they can't show you more photos or pictures of themselves. Yes ☐ No ☐
- They delay meeting in person or talking with you on a video chat. Yes ☐ No ☐
- When you arrange to meet this is often cancelled or postponed last minute due to an emergency. Yes ☐ No ☐
- When you speak to them, their accent matches their stated age, origin, photographs. Yes ☐ No ☐
- Images appear to have been professionally taken. These are highly posed and contain shots of puppies, mountains, military regalia or uniform. Yes ☐ No ☐
- Do they seem too good to be true? (Looks, wealth and personality). Yes ☐ No ☐

The above Information was taken from the romance fraud questionnaire DC-RomanceFraud 022021

Cost of living scams

> With the cost-of-living crisis impacting people all over the UK, criminals are taking advantage of the financial hardship and government grants to scam people out of their hard-earned money.

Cost of living payments

Beware of fake text and emails relating to the cost of living and energy crisis. The government is offering help for households but criminals are also pretending to offer support schemes. Such texts and emails may look official and pretend to be from gov.org, HMRC or DWP. **You don't need to apply or do anything else to claim the payment.**

Examples include:

- Fake cost of living related grants
- Fake cost of living relief funds
- Fake council tax reductions, rebates, or refunds
- Fake tax rebates from HMRC
- Fake offers of assistance to help with universal credit applications

Fake Loans

With costs rising around us, more people will be looking to take out a loan, be sure to borrow from a legitimate company and be aware of criminals and them often 'too good to be true' offers.

These scams offer guaranteed loans that require you to pay an upfront fee for the loan. Once the fee has been paid, you do not hear from the criminals again and the loan is never received.

Stay safe

- You do not need to apply for this support, if you are eligible, you will automatically receive these payments.
- You **will not** be contacted by the Government or Ofgem asking you to share your bank details to claim this benefit.
- Don't click on a link sent to you out of the blue, even if it looks legitimate. Go to the official website for the information, or for the correct contact details to get in touch yourself.
- Scammers often pose as authorised firms to gain a victim's trust, if you are asked to pay an upfront fee before your loan can be funded as an 'admin fee', a 'deposit' or 'because you have bad credit' this could be a scam.
- Never pay loan fees using gift cards like iTunes, Google Play or Amazon.

Always **Stop.Think.Tell.** before giving any information. A genuine firm will never pressure you into an immediate decision. This simple action could save you hundreds of pounds.

Selling Site Scams

> **Popular online marketplaces such as Facebook Marketplace, Gumtree and ebay, can be great for buyers and sellers alike, however there are also plenty of scammers posing as genuine customers and merchants.**

Unfortunately, social media makes it easy for scammers to pose as someone else, fraudulently list items and steal from unsuspecting buyers.

Here are some red flags for selling site scams

Sellers offering suspiciously low prices for high value items
A buyer making accidental overpayment for a product
Requesting initial deposit for an item to be held
Asked to send the item before payment is received
Request to send courier for collection of goods
Requesting payment outside of the preferred payment platform

Stay Safe

- Do not send items before receiving payment. Always check you have received payment into your bank account or preferred platform by logging into the account via an official website or app. Do not trust screenshots or receipts showing successful payment sent to you by the buyer.
- Beware of buyers claiming to have accidentally overpaid for an item. Many scammers use stolen cards, fake PayPal accounts or counterfeit funds to send payment and claim

a mistake is made and request a refund. Eventually the payment will be recalled, and you will have lost the item you're selling and your own funds.

- Scammers may tell you that an item is getting a lot of attention and they require a deposit to "secure" the item. Chances are they might be telling the same thing to tens or even hundreds of others, collecting deposits and stringing you along.
- Take a close look at the user profile. Always check the buyer or sellers' profile, check the date the account was created and read previous reviews, if they haven't sold anything before be wary of making that transaction.

If it's to good to be true, it probably is.

Beware of anything that's for sale for a fraction of the retail price. Scammers may try and make you feel like you need to act immediately or miss out on a good deal. High pressure tactics can make a buyer act irrationally and hand over cash or potentially give out information they shouldn't.

Before rushing to grab a bargain or make a sale, remember Claude and **Stop.Think.Tell.**

By stopping to verify the seller or buyer you could be saving yourself money, time and stress by avoiding a scammer.

Delivery charges Phishing email and texts

Emails or text are sent stating there is an outstanding delivery charge or additional postage payment or missed delivery schedule charged for a small fee.

There will be a link to click on where you are directed to pay the fee, thereby giving the criminals your bank details.

Stay safe

- Have you ordered something recently? Keep track of receipts/confirmation emails for online purchases.
- Do not click on the link within the message. Go to the retailer's actual website and check on the status of your delivery.
- If a message is asking for money or personal or financial information in exchange for a package it's likely to be a scam.
- Fraudsters can spoof email addresses/ telephone numbers, so don't assume the link given is to a genuine website.

WhatsApp friends and family crisis

Phishing email and texts

> **Messages are sent purporting to be from a relative or friend from an unknown number.**

They claim their phone has been damaged, lost or stolen which is why they are using a different number. In some cases, correct names are being given, but this may just be luck rather than them knowing the name of your relative or friend!

The messages request to borrow money or pay for something (with a link in the message) stating that the alleged change in phone number means they can't access their usual online banking. They will also give some sort of excuse as to why the money can't be paid into their own account, so will give banking details of someone else.

Stay safe

- Always verify requests in person or verbally to ensure you are speaking to the person that you think you are.
- If you receive a message like this, try contacting your loved one by calling the number you already have, not the 'new' one on WhatsApp.

Online shopping

> Online shopping and auction sites can save time, effort, and money.
>
> Millions of people use websites to buy new or second-hand goods for competitive prices with the opportunity to purchase a huge choice of goods from all over the world.

Because buyers and sellers rarely meet, when you make a purchase or sale on a website, you are reliant on the security measures of the website.

Always be wary if you are encouraged to move away from the website to complete any transaction, even if you are being offered a discount to do so! By communicating and paying away from the website, contrary to the policies, you risk losing any protection you had.

If you are selling goods, before posting any item, log onto your account via your normal method and not a link given by the buyer to check you have received the money.

Be careful of what address you send items to. Fraudsters may ask you to send items to other addresses. If you send the item to an address other than the one registered on the user account, you may not be provided any protection from the website or payment service.

It is a good idea to use a credit card when shopping online. Most major credit card providers protect online purchases and are obliged to refund you in certain circumstances. If something does go wrong your main bank account won't be directly affected if you use a credit card rather than a debit card.

Check to see if there is a closed padlock in the browser bar when you come to pay for your goods. This doesn't guarantee that the retailer is legitimate, but it does mean the connection is secure. Don't use the site if you cannot confirm the connection is secure.

Stay safe

- Stay on the website payment methods.
- Do your research on the buyer/seller and read the consumer advice on any website you are using to make a purchase.
- Be wary of offers that look too good to be true.
- If you are selling online, be wary of emails stating funds have been sent. Always log into your account via your normal route (not via link) to check the payment status.

Buying pets online

> **Buying a pet online can be very difficult and there are various frauds you could open yourself up to.**
>
> **This can be around transportation, but there are always laws around buying and selling certain types of animals that means you really need to do your research before committing to a purchase.**

Lucy's law means that anyone wanting to get a new puppy or kitten in England must now buy direct from a breeder or consider adopting from a rescue centre instead. It also means that licensed breeders are required to show puppies interacting with their mothers in their place of birth.

Stay safe

- When purchasing a pet, never give a deposit up front until you have seen the animal and are quite happy that what you are purchasing is what you want.
- You can no longer buy a puppy or kitten in England from a third party (someone who is not a breeder) that is under the age of six months old, see Lucy's law.
- Beware of adverts stating they will courier the pet to you and wanting costs upfront. Do your research before parting with your money. There are companies that do courier pets, it is advisable to check what company are doing the transport and contact that company yourself to verify the sale and transportation.
- Always be wary if the puppy has a foreign pet passport as puppies must be over the age of 15 weeks old to enter the UK legally.

- No matter what animal you are buying make sure you research as to who you are buying from and that they are legitimate sellers.

If buying a puppy visit:
www.dogtrust.org.uk/help-advice/buyer-advice

Can't resist those puppy dog eyes?

Do your research - always try to buy your pet from a rescue centre or reputable breeder

Scam protection

Ten top tips to keep you and your devices secure

> **Criminals are experts at impersonating people, organisations and the police. They spend hours researching you hoping you'll let your guard down for just a moment.**

They can contact you by phone, email, text, letters, on social media, or in person. They will try to trick you into parting with your money, personal information, or buying goods or services that don't exist.

1. **Verify any unexpected contact is genuine by using a known number or email address to contact organisations directly.**
   Is this caller who they say they are? After hanging up, wait five minutes and make sure you can hear a dial tone before making any other calls, or use your mobile. **Never allow** an unsolicited caller remote access to your computer or devices.

2. **Don't be pressurised into sending money.**
   Stop, think and check with a trusted source or person. It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you. Have confidence in yourself, if it feels wrong to you – it probably is.

3. **Use someone you know and trust for shopping & other essentials.**
   Don't hand money over to someone on the doorstep.

4. **Authorities like the Department for Work and Pensions (DWP) and Her Majesty's Revenue and Customs (HMRC) will never ask for banking details like your password or PIN on the phone or in person.**
   You will **never be asked** to move money to a 'safe account'. Police or banking representatives will never ask you to help in an investigation by moving money or withdrawing funds.

5. **Check IDs and get them verified.**
   Genuine officials will be more than happy to wait while you verify their ID.

6. **Pick strong passwords.**
   Choose three random words with a mixture of upper/lower case, numbers and special characters. Do not use the same password across sites. Enable Two Factor Authentication (2FA) on your accounts and devices that offer it, this provides a second layer of security.

7. **Be wary of phishing scams.**
   Don't click on any links or attachments in unexpected emails.

8. **Regularly review your social media settings.**
   For those of you who use social media, make sure that it is set up correctly, review your privacy settings to ensure your profile is appropriately locked down.

9. **Use anti virus and ensure you are using the latest versions of software, apps and operating systems on your phones, tablets, desktops and laptops.**
   Update these regularly or set your devices to automatically update so you don't have to worry.

Scam protection continued

10 **Backups.**
Always back up your most important data such as your photos and key documents to an external hard drive and/or cloud storage.

Report suspicious texts by forwarding them to **7726**, which spells SPAM on your keypad.

If you think you've received a phishing email forward to **report@phishing.gov.uk**

If you think you've fallen victim to a scam contact your bank immediately and report it to Action Fraud by visiting **www.actionfraud.police.uk** or calling **0300 123 2040.**

The role of Action Fraud

> **Action Fraud is the national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cybercrime in England, Wales and Northern Ireland.**

Reports can be made any time of the day or night using the online reporting tool. Reporting online is quick and easy. The tool will guide you through simple questions to identify what has happened and advisers are available on web chat 24 hours a day to give you help and advice if you need it. When you report to us you will receive a police crime reference number. Reports taken are passed to the National Fraud Intelligence Bureau. Action Fraud does not investigate crimes.

How your crime report is assessed

Reports to Action Fraud are considered for assessment or referral to the police or other law enforcement agency by the National Fraud Intelligence Bureau, operated by the City of London police.

Once reports have been recorded by Action Fraud, they are assessed against Home Office counting rules, which are the standards against which police record crime. Data matching allows reports from different parts of the country to be linked through analysis. Reports are then triaged to determine those that are highest risk, threat, or harm.

These triage reports are assessed by experienced crime reviewers who consider the viability of each report, or series of reports where these appear to be linked.

The role of Action Fraud continued

This viability test is to ensure there are definitive lines of enquiry for a force, or other law enforcement agency to progress. Crimes that meet the viability test are referred to the appropriate police or law enforcement agency for action. The recipient may not always be your local police force.

Information you provide on the bank accounts, websites and phone numbers used by fraudsters is regularly provided to industry partners so they can stop them from being used against future victims.

Not every report results in an investigation, but every report helps to build a picture of offending and is retained for future intelligence.

How you obtain an update on the progress of your report

If you have registered on the Action Fraud system as a victim or proxy reporter, then you will receive automatic updates to your individual account. You will also receive postal updates.

If you wish to seek an update outside of the above, or if you have not registered with Action Fraud, then an update can be requested through the 'contact us' facility on the Action Fraud website.

If your report is disseminated to a force, you will be provided with the name of the recipient force. Once your report has been disseminated, the recipient force takes responsibility for providing you with updates on the progress of your case.

What happens once your report has been referred to a police force

Each police force (or other law enforcement agency) will review and assess referrals from the National Fraud Intelligence Bureau. They will triage the reports based upon threat, risk and harm and local priorities set by their Police

and Crime Commissioner. You will be provided with regular updates on the progress of your report.

If a force decides no further action will be taken, they will communicate this to you with a rationale for their decision.

Options to seek civil redress

In cases where criminal investigations are not carried out or do not lead to a conviction, you may wish to consider other options to recover your losses. There are civil asset recovery agents who may be able to act on your behalf to recover criminal assets that represent some or all your losses.

Before choosing a civil asset recovery agent, you should undertake adequate checks to ensure they are legitimate. The financial conduct authority has details of known fraudulent civil asset recovery agents.

Should you choose to engage a civil asset recovery agent, you should update your Action Fraud report with their details. This update can be made to your individual account or through the contact us facility on the Action Fraud website if you have not registered with Action Fraud.

Contacts

Action Fraud
☎ 0300 123 2040
www.actionfraud.police.uk

Age UK
☎ 0800 169 8787
www.ageuk.org.uk

CIFAS
www.cifas.org.uk

Citizens Advice Bureau (CAB)
☎ 03444 111 444
www.citizensadvice.org.uk

Companies House
www.gov.uk/government/organisations/companies-house

Crimestoppers
☎ 0800 555 111
www.crimestoppers-uk.org

Cyber Aware
www.cyberaware.gov.uk

Financial Conduct Authority (FCA)
☎ 0800 111 6768
www.fca.org.uk

Friends Against Scams
www.friendsagainstscams.org.uk

Get Safe Online
www.getsafeonline.org

Have I Been Pwned
www.haveibeenpwned.com

Mail Preference Service
☎ 020 7291 3310
www.mpsonline.org.uk

National Cyber Security Centre
www.ncsc.gov.uk

Online Dating Association (ODA)
www.datingagencyassociation.org.uk

Think Jessica
www.thinkjessica.com

Trading Standards
☎ 0808 223 1133
www.nationaltradingstandards.uk

UK Finance
www.ukfinance.org.uk

Victim Support
☎ 0333 3007150
www.victimsupport.org.uk

Financial Ombudsman
www.financial-ombudsman.org.uk

DERBYSHIRE ALERT

Sign up today

...to be aware of crime updates and local policing news in your area

Derbyshire Alert is a free two-way community messaging service that allows Derbyshire Constabulary to send out messages on local crimes, good news, community events and crime prevention.

Log on and sign up to create your profile at:
www.derbyshirealert.co.uk
to receive emails, and urgent messages by text and voice mail.

Making Derbyshire Safer **Together**

DERBYSHIRE CONSTABULARY

Final reminder

Postal

If it sounds too good to be true, then it probably is. You can't win a lottery or a prize draw if you haven't entered it.

Telephone

Beware of cold callers. Never talk money or give other personal details over the phone. Hang up and wait five minutes. Use only telephone numbers you can verify yourself, not those given to you by the caller. Remember number spoofing.

Doorstep

Not sure? Don't open the door. Check their credentials before you let them in if you are expecting them.

Online

Check the web address, never click on unsolicited links. Be wary when dealing with a company who suddenly want to change the account details for where your payment is going. Remember email spoofing.

Always think of Claude and **Stop.Think.Tell.**

By taking a moment to pause, think about a request and talk to someone you trust, you can help us to #SockItToTheScammers.

☎ 101 non-emergency, in an emergency always call 999

@DerbysPolice | derbyshireconstabulary

www.derbyshire.police.uk

Making Derbyshire Safer **Together**

Fraud your essential guide-Booklet A5 06-2023