Fraud

Your Essential Guide...

When in full screen mode press Esc to exit

Lincolnshire Alert

Free Community Messaging Service for Lincolnshire residents

Keep informed Stay safe Have your say

- Receive crime reduction and community safety alerts direct to your email inbox
- Have your say about policing where you live
- Choose what information you want to receive

Sign up today to receive important, localised information

LINCOLNSHIRE ALERT

Lincolnshire POLICE & CRIME COMMISSIONER
SAFER TOGETHER

www.lincolnshirealert.co.uk

Where can I get help if I've been the victim of crime?

Victim Lincs

TALK TO US

01522 212333
Monday - Friday
8am - 4pm

victimlincs.co.uk

If you've been the victim of crime, Victim Lincs can help - whether you choose to report the crime to the police or not.

We can:

Inform
Answer any queries or concerns that you may have, as well as provide practical advice and information

Support
Discuss the support options available and, should you need further support, make a referral to the specialist service most suited to you

Listen
We are independent to the police, so anything you tell us will be in confidence*

Lincolnshire POLICE & CRIME COMMISSIONER
SAFER TOGETHER

*unless there is a risk of harm to yourself or others, or where there is a legal requirement

Contents

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 underreported 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 the four fraud enablers, and they are:

- Telephone,
- Doorstep,
- Postal, and
- 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 Lincolnshire with practical advice on how to spot the fraud, and what to do to prevent you from becoming a victim of that type of fraud.

Spoofing

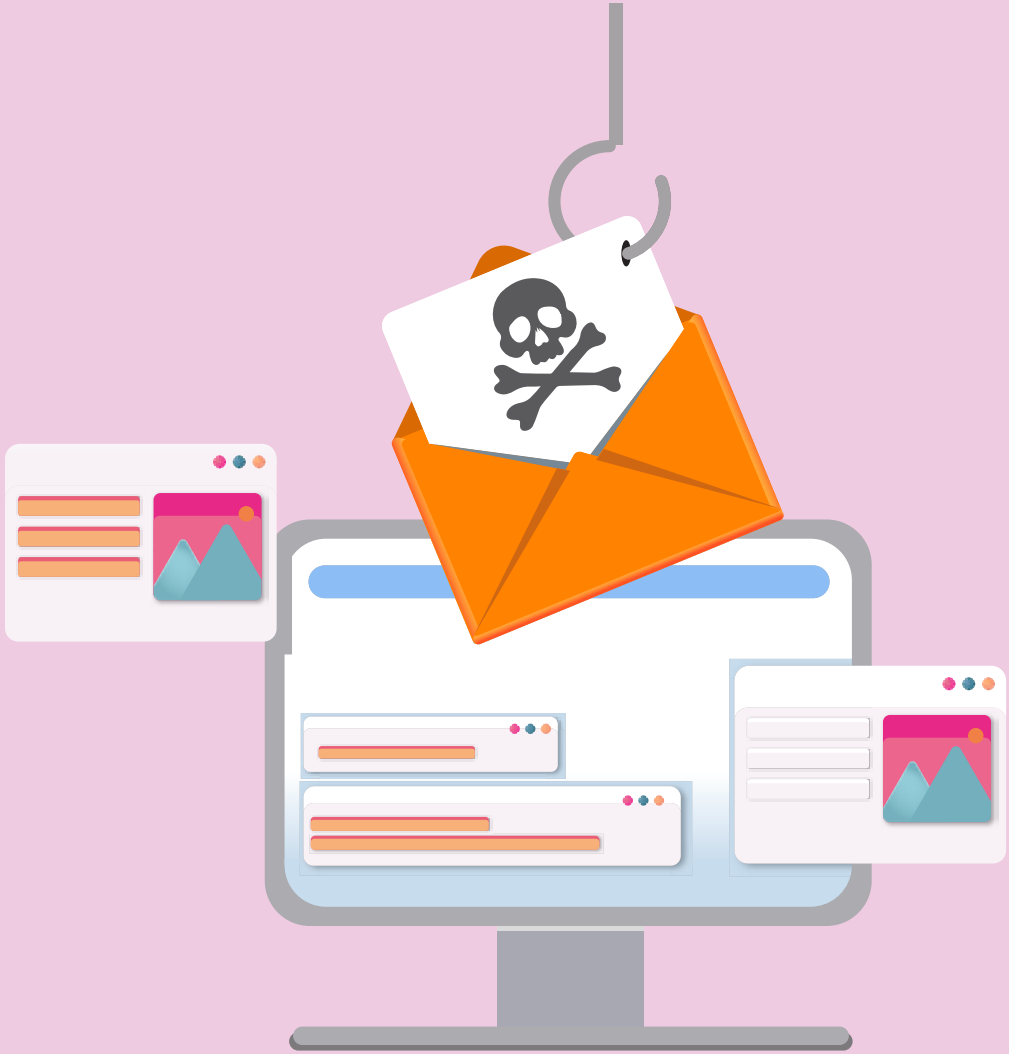
Phone numbers and email addresses can be spoofed by criminals to appear as though they are from someone, or somewhere, other than the actual source.

Email and telephone spoofing tools are widely available, and criminals often use them as part of phishing attacks. Because the spoofed 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 that someone is who they say they are.

- Be suspicious if someone tries to draw your attention to the email address or telephone number displayed as a means 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 pension. 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 so you can 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 if they ask for passwords or your date of birth.
- 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 been a victim of, 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 their 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 being 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 passcode – 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 are 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 to 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'll 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 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 service 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 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 Fraud

Many victims of fraudulent mail, also known as mass market 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 fraudulent 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 your 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 fraudulent 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.

STAY SAFE

- You cannot win a prize if you haven't entered
- Be wary of anyone asking you for your private information
- Ask yourself 'Why am I being asked to make payments?'

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 also laws around buying and selling certain types of animals that means you really do 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 dog 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 6 months old, see Lucy's Law.
- Beware of adverts stating that they will courier the pet to you and wanting costs up front. Do your research before parting with your money. There are companies that do courier pets, so it is advisable to check what company are doing the transport and contact that company yourself (not from a link from the seller) to verify the sale and transportation.
- If buying a puppy see; www.dogstrust.org.uk/help-advice/buyer-advice
- 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 a legitimate seller.

Impersonation Fraud (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 or 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 they will then collect from you for ‘evidence’. They may claim the money could be counterfeit, or that they are 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 a courier.
- Asking to purchase other items, like gift cards or vouchers.
- In all these cases they will assure you that you will soon be reimbursed.
- Fraudsters want to avoid detection, and may give you instructions to achieve this such as;
- Informing you it is an undercover operation involving 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, e.g. the money / 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, bank card, 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 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 overcharged for any work done.

They can use deception to convince you by;

- Claiming they were working on a neighbours' address and noticed you need 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 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.

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 your 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 and unattended, so a second individual can't enter without your knowledge.

Thinking of having work done on your home?

To help you save time, money and stress when you're preparing to get building work, renovations or repairs done on your home and avoid problems. Consider these tips:

- Speak with multiple tradespeople to compare.
- Check with your local council to see if you need any permission or approval.
- Ask for a contract for the work.
- Check with friends and family for recommendations, or reviews on legitimate trader websites.

Consumers often turn to the internet and social media to find a trader. Criminal traders may use popular trader matching platforms or social media to advertise their services.

Many trade associations recommend obtaining at least three quotes from traders before agreeing to any work on your home. If you're being pushed to take on a trader quickly, this could be a sign that something isn't right. Check out how to find a trader – Before you get building work done - Citizens Advice

Don't suffer regret when improving your home, get advice before you start!

If you're not sure, research more! Visit Consumer - Citizens Advice or call 0808 223 1133 for more information.

Safe Accounts

DON'T BECOME A VICTIM

Fraudsters cold call you pretending to be from your bank. They claim there is an issue with your bank account where it has been compromised and they need to open a new account. They will convince you this is necessary so they can transfer your money from your old account into the new one they have opened for you. They may refer to it as a 'Safe Account'.

This type of call usually comes after a text message you may have received, such as a missed parcel delivery. In many cases, people have clicked on a link in those text messages and filled out information such as personal details or even bank account details.

The fraudsters will tell you that because you have clicked on that link, and entered personal details, you have compromised your bank account, and they will now need to open a new account for you.

They can convince you this is genuine because they will be using the information you gave when you clicked on the text message link you received previously.

They may also spoof the number they are calling you from so it looks like its close to or is your banks telephone number. They may say it's not the exact number, as they are ringing from a different extension number.

STAY SAFE

- There is no such thing as a safe account.
- If you receive an unexpected call like this, then think about any suspicious text messages you may have received previously. Hang up the phone and either wait to clear the line, or use another phone to call your bank on a number you can verify yourself, not the one given to you by the caller.
- Ask yourself, 'How do I know they are who they say they are'.

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.

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 investments. Indeed, emerging investment markets may be unregulated, making these open to abuse.

Companies may be registered at prestigious addresses. This does not mean they operate from there. It is an accepted business practice to rent such a virtual office to enhance a business's 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' or 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're investing in is real, it could be fraud. Check the FCA register before investing.

www.fca.org.uk/scamsmart

Financial Abuse of Power

Financial abuse is a type of abuse which includes:

- having money or other property stolen,
- being defrauded,
- being put under pressure in relation to money or other property
- having money or other property misused

Financial abuse is a crime. What financial abuse looks like can vary, which can make it difficult to identify. There are signs you can look out for, either for yourself or for a friend or family member. Here are some of the signs that someone might be a victim:

- Have you noticed unusual or inappropriate transactions on your bank statements?
- Are you unable to access cash, either via banking or income sources, such as your pension or other benefits?
- Are you being pressured into giving your money to others, leaving you without the money you need to pay for essentials?
- Have you recently lost money without any explanation?
- Have you lent money to someone and they haven't given it back?
- Do you feel pressured or forced into making changes to your will or other financial plans?

Financial abuse can be committed by someone you know such as a family member taking advantage of a power of attorney relationship, a carer keeping your bank card after doing your shopping or a fraudster coercing you into transferring money to them. More examples can be found at the Hourglass UK website – a charity who aim to stop abuse in Older people. You can call their 24 hour helpline on 0808 808 8141.

Financial abuse often occurs alongside other forms of abuse. Vulnerable people are at particular risk of financial abuse. If you want to find out more you can also visit the Age UK website.

If you have a concern about an adult with care and support needs call:

- Adults safeguarding - 01522 782155 (Monday to Friday, 8am to 6pm)
- or 01522 782333 (outside office hours)

You do not need to know everything about the situation. You may just be worried or feel that something is not right.

If you believe that a crime has been committed and there is an immediate risk of danger, call the police on 999 or 112.

If there is no immediate danger, call the police on 101.

Domestic Abuse and Fraud

This is often part of wider economic abuse, and it is often linked to other forms of abuse such as coercive and controlling behaviour, physical, sexual, emotional abuse or stalking & harassment.

Domestic abuse related fraud can be linked to various types of fraud mentioned in this booklet.

Identity fraud can be used by users to take control of your finances and apply for credit using your details. You may feel in fear of challenging or reporting this at the time or coerced into going along with this. Abusers can also use these details to hack online accounts such as social media or online shopping accounts.

If a victim becomes a money mule, this allows the abuser to carry on illegal activity using your details. You may feel completely controlled and coerced into providing them with your personal details and use of your bank accounts. Some abusers may tell you that they cannot have their own bank account and therefore need the use of yours. This is another controlling tactic to have contact with your abuser, allowing them access to your account, seeing what you have spent money on which can feed into further controlling and possessive behaviour.

The start of an abusive relationship may begin with romance fraud, telling you their personal details you believe are true and finding yourself so engulfed in their lies that you no longer know what to believe. Sometimes abusers will start off like this, infiltrating your life and before you know it, they are living with you and your life is consumed by them.

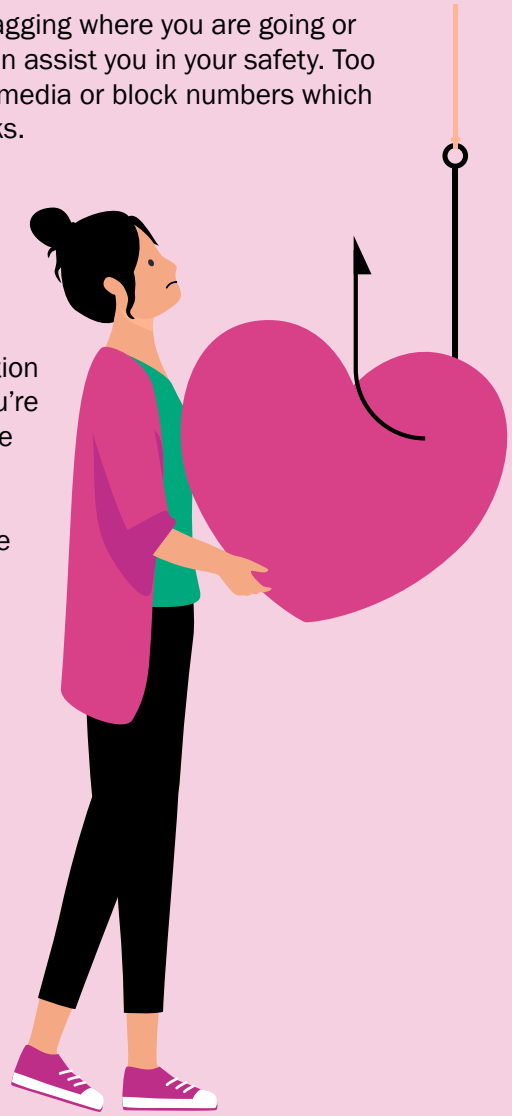
Abusers may often pretend to be someone else to gain further information from you. They may set up fake profiles on social media or use alternative contact numbers or email addresses to further stalk and harass you. They may even entice third parties to further abuse you, pretending they are a school or doctor for example so that you give personal information or attend an appointment where they then meet you.

By keeping your online profiles private, not tagging where you are going or uploading pictures with known landmarks can assist you in your safety. Too many people feel they must come off social media or block numbers which can further isolate you from support networks.

Banks across England and Wales are aware of the links to finances and domestic abuse and can often support you if you have concerns regarding your accounts. Look to visit a branch or call them to find out more.

Under Clare's Law you can apply for information about your current or ex-partner because you're worried that they may have a history of abuse and are a risk to you or request information about the current or ex-partner of a friend or relative because you're worried they might be at risk.

Request information under Clare's Law: Make a Domestic Violence Disclosure Scheme (DVDS) application | Lincolnshire Police (lincs.police.uk)



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 the 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 communication off the dating website. 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 they will pay it 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.
- Do your own research on the person – are they members of any other social networking sites? Can you confirm what they are telling you about themselves, such as where they work or where they live?
- 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.
- 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

Ponzi Schemes 

Ponzi schemes are 'get rich quick' investment scheme which pay returns to investors from their own money, or from money paid in by subsequent investors. There is no actual investment scheme as the fraudsters siphon off the money for themselves.

A fraudster places an advertisement for a non-existent investment that offers extraordinary returns in a short space of time. After receiving the promised returns on their investment, the first investors start to spread the word to family and friends. In this way, the scheme gains credibility.

Because the money isn't invested in any kind of investment vehicle, there are no profits. Instead, the first investors are simply paid out from the money paid in by new investors.

Ponzi schemes are created for all levels of income.

Typically, the fraudster will vanish with investors' money, so the system eventually collapses with later investors receiving nothing – including their initial investment.

Because Ponzi schemes are unauthorised and make no profits, you are very unlikely to recover any lost money.

STAY SAFE

There's no such thing as a 'guaranteed risk-free' investment. High returns can only be achieved with high risk

- Be wary of hard-sell techniques – don't be pressured into making rushed decisions.
- Be wary of things such as glossy brochures, dazzling language such as 'high yield investment programme', mock websites and extravagant venues. Investigate the company's status and contact details yourself.
- If you're not sure the company you're investing in is real, it could be fraud. Check the FCA register before investing.

www.fca.org.uk/scamsmart

Pyramid Schemes

Pyramid scheme fraud involves an unsustainable business which rewards people for enrolling others into a business that offers a non-existent or worthless product.

A fraudster advertises a multi-level investment scheme that offers extraordinary profits for little or no risk.

You're required to pay a fee to enter the investment scheme.

You're then required to recruit friends or family members to enter the scheme. If you do this successfully, you're paid out of their receipts. They are then told to recruit others to keep the chain going.

Your money is not actually invested in any product. Instead, it's simply passed up the chain of investors. Because pyramid schemes are unauthorised and make no profits, you're very unlikely to recover any lost investment. While the fraudster at the top will collect most of the profits, those who entered the scheme later end up losing out.

Legitimate trading schemes rely on valuable goods and services, while illegal pyramid schemes focus simply on recruiting more and more investors.

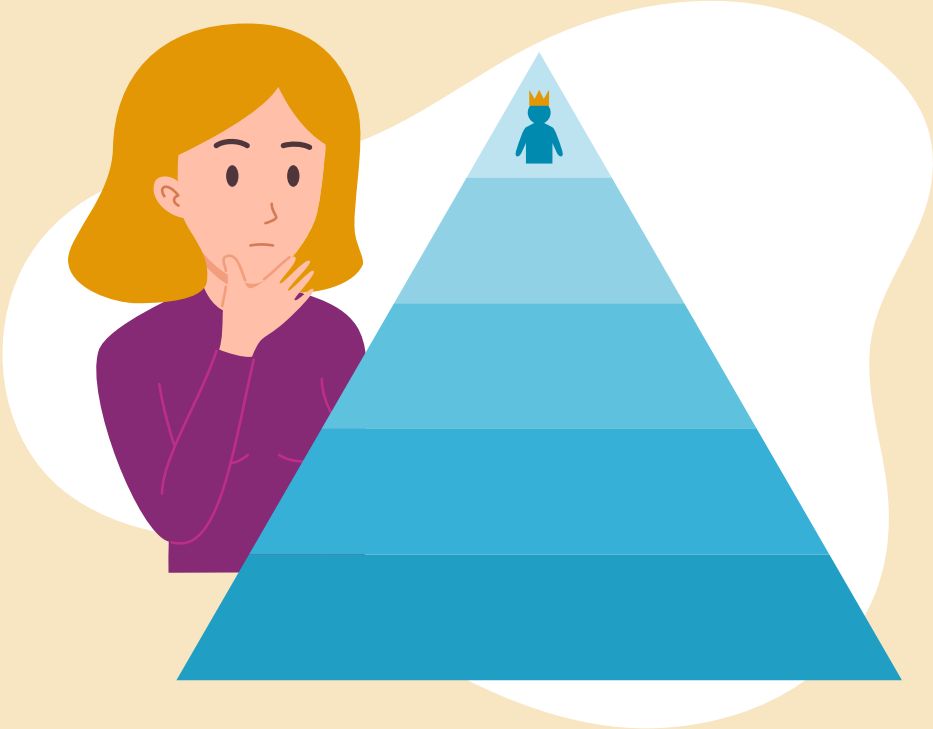
Using hard-sell techniques, fraudsters try to pressure you into making rushed decisions, giving you no time to consider the nature of the investment.

Fraudsters aim to make their business seem legitimate. This means they will often use technical jargon, impressive job titles and mock websites to look credible. If you have any suspicions about a scheme's authenticity, you should investigate the company's status and contact details.

STAY SAFE

If you're considering any type of investment, always remember: if it seems too good to be true, it probably is. High returns can only be achieved with high risk.

Pyramid schemes often involve products that are overpriced and have no real resale value. You should think about the true value of your investment before convincing friends and family to join the scheme.



Delivery Charges – Phishing Email and Texts

Emails or texts are sent stating there is an outstanding delivery charge or additional postage payment or a missed delivery reschedule charge at 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 Retailers 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 its' likely to be fraud
- Fraudsters can spoof email addresses, 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 temporarily 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 bank 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 a 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 transactions, even if you are being offered a 'discount' to do so! By communicating and paying away from the website, contrary to their policies, you risk losing any protection you had.

If you are selling goods, before posting any item, log into your account via your normal method (not a link given by the buyer) and 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's a 'closed' padlock in the browsers 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!
- Be wary of any requests to pay by bank transfer or virtual currency instead of the websites recommended 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

SIM Swapping

In today's digital world, our mobile phones are more than just communication tools - they're gateways to our most sensitiveinformation. Unfortunately, this makes them prime targets for cybercriminals. One of the most alarming tactics currently on the rise is SIM Swapping, a form of identity theft that can lead to devastating financial and personal consequences.

WHAT IS SIM SWAPPING?

SIM swapping is a type of fraud where criminals trick your mobile provider into transferring your phone number to a SIM card they control. Once they have access to your number, they can intercept your calls and text messages—including two-factor authentication (2FA) codes used to secure your online accounts.

With control of your phone number, attackers can reset passwords, gain access to your email, bank, and social media accounts, and even lock you out of them entirely. This scam is not new, but recent months have seen a sharp increase in reported cases, with many victims suffering significant financial losses.

WHICH ACCOUNTS ARE AT RISK?

In short: all of them. However, the most vulnerable and valuable targets include:

- **Email accounts** – Often the key to resetting passwords for other services
- **Banking and financial apps** – Direct access to your money
- **Social media accounts** – Can be used for scams, impersonation, or extortion

Criminals are constantly finding new ways to exploit any online account that can be monetized or used for further fraud

HOW TO TELL IF YOU'VE BEEN TARGETED

Here are some warning signs that you might be a victim of SIM swapping:

- **Sudden loss of mobile service:** If your phone stops receiving calls or texts unexpectedly, it could mean your number has been transferred to another SIM
- **Unusual account activity:** Notifications about logins or SIM activations you didn't initiate are red flags
- **Locked out of accounts:** If you can't access your email, bank, or social media accounts, someone else might have taken control
- Unauthorised transactions: Unexpected charges or withdrawals from your bank account could indicate fraud.

If you notice any of these signs, contact your mobile provider and bank immediately.

HOW TO PROTECT YOURSELF FROM SIM SWAPPING

While no method is fool proof, there are several steps you can take to reduce your risk:

1. Use strong, unique passwords for each of your accounts. Consider using a password manager to keep track of them
2. Enable app-based 2FA instead of SMS-based codes. Common Apps include Google Authenticator, Apple Authenticator and Microsoft Authenticator

3. Add a PIN or password to your mobile account. Most carriers allow you to set a security PIN that must be provided before making changes
4. Limit personal information shared online, especially on social media. Criminals use this data to impersonate you
5. Stay alert to phishing attempts. Don't click on suspicious links or provide personal information to unknown sources
6. Monitor your accounts regularly for any signs of suspicious activity.

WHAT TO DO IF YOU'RE A VICTIM

If you suspect you've been targeted or compromised:

- Contact your mobile provider immediately to regain control of your number
- Notify your bank and other financial institutions to freeze or monitor your accounts
- Change your passwords for all important accounts, especially email and banking
- Report the incident to Action Fraud, the UK's national reporting centre for fraud and cyber crime where you should report fraud if you have been a victim

FINAL THOUGHTS

SIM swapping is a serious and growing threat, but with awareness and proactive security measures, you can significantly reduce your risk. Stay informed, stay vigilant, and take steps today to protect your digital identity.

What to do if Your Bank Card is Stolen

If your bank card is stolen, we would encourage you to carry out the following actions;

- If you have mobile banking, cancel the card in your App. If you don't have mobile banking, contact your bank as a matter of urgency for them to cancel the card and issue you with a new one
- Check for any unusual transactions and ensure you update your bank with anything you don't recognise
- Check your direct debits. Some direct debits are updated when a new card is issued automatically. If your stolen card has been used to set up any new direct debits that are not yours, these will be updated with your new card details, so you need to ensure these are cancelled by contacting the company concerned

What to do if Your Mobile Phone is Stolen

If you have your phone stolen, we would encourage you to carry out the following actions:

- Contact your bank as a matter of urgency to prevent transactions being made or loans being taken out
- Freeze or cancel bank accounts associated to the handset
- Force all devices and applications to log out of your accounts. This should include email accounts which can be used by criminals to reset other passwords.
- Block your phone from another device as soon as possible
- Notify your phone provider that your phone has been stolen so that 2FA messages do not get sent to this number

Mobile Phone Contract Fraud

What happens;

Victims are offered early handset upgrades, or new contracts, at significant discounts. Once customers have been convinced that the deals are genuine and agree to proceed, suspects then ask for their online mobile account credentials, including log-ins, address and bank account details.

Suspects then place orders with genuine companies on behalf of victims, however select a different handset to that requested and have it shipped to the customer's address.

Upon receipt, suspects assure victims that this has been an error and instruct them to 'return' the handset to a different address not affiliated to the mobile company. These addresses are usually residential.

After intercepting the 'returned' handsets, the suspects cease contact, and victims find themselves stuck with no phone and liable for the entirety of a new contract taken out in their name.

What you need to do

- Cold calls about mobile upgrades and contracts - If you're unsure that the person calling you is an official representative of the company they claim to be from,
  hang up and do not reveal any personal information.
- Only contact your mobile network provider on a number you know to be correct. For example,
  191 for Vodafone customers, 150 for EE customers, 333 for Three customers, 202 for 02 customers, 4455 for Tesco Mobile, 789 for Virgin Mobile and 150 for Sky Mobile.
- If you receive a device that you did not order or expect, contact the genuine sender immediately. The details for this will be within the parcel.
- NEVER post a device directly to a given address. All genuine Mobile Network Operators would send out a jiffy bag for you to return without you incurring additional cost.


Crypto Dream
Scam Nightmare
Ten tips to avoid losing thousands of pounds to fraud
Avoid becoming a victim of Crypto Investment Fraud
1 Do not respond to unsolicited approaches on social media or dating platforms about day trading or crypto investment schemes
2 Refuse the offer to be a 'member of an exclusive club' from a financial 'professor' or 'guru'
3 Beware of 'early exit' attempts to move communication from the original platform onto an encrypted platform, such as WhatsApp or Telegram
4 Do not believe exceptionally high returns on your investment in a short period of time
5 Do not be convinced if a small initial withdrawal is successful; you may be blocked from making any further withdrawals by high fees or taxes
6 Do your own research; criminals create fake platforms to imitate genuine investment sites. Search the company on the FCA Firm Checker. Beware of poor design, grammar and spelling
7 Be cautious if communication with a representative sounds like a Chat Bot or AI generated
8 Do not allow a third party to listen in or advise you on what to say when opening a new account on a crypto exchange
9 Beware of continuous pressure to make additional investments, and of messages being sent outside of business hours
10 Be suspicious if you are advised to ignore warning messages from banks & crypto exchanges or being instructed not to tell anyone about the 'special deal'
Losing money through Crypto Investment Fraud is not a genuine trading loss, your money has been stolen.
If you think you have been a victim of Crypto Investment Fraud, report it to Action Fraud.
NCA National Crime Agency
STOP THINK FRAUD
www.nca.gov.uk

Ten Top Tips to Keep You and Your Devices Secure...

1. Verify any unexpected contact is genuine by using a known number or email address to contact organisations directly (please do be aware of spoofing). 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 a mobile phone. 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 okay 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 and 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. They will never ask for money or 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. Create a separate email password. If a hacker gets into your email, they could get into all your accounts that are linked to it. Make sure you have a strong password and make sure its different to all your others. Save passwords in your browser. Your internet browser will often give you the option to remember your passwords for you. This is a safe way to store your passwords, helping you to create strong and different passwords without having to remember them all.
7. Be wary of phishing. Don't click on any links or attachments in unexpected emails.
8. Social Media. 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 antivirus and ensure you are using the latest version 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.
10. Backups. Always back up your most important data such as your phones and key documents to an external hard drive and / or cloud storage.

THE NATIONAL CYBER SECURITY CENTRE

The National Cyber Security Centre (NCSC) Cyber Aware website provides simple, trusted advice from the UKs NCSC on how to stay safe online and protect yourself from cybercrime.

This QR code will take you to their website and is safe for you to use. Hover over the code with your camera and follow the link

VISIT WWW.NCSC.GOV.UK/

Contacts...

Report Fraud

Call 0300123 2040 or visit www.reportfraud.police.uk

Age UK

Call 0800 169 8787 or visit at www.ageuk.org.uk

Cifas

Visit www.cifas.org.uk

Citizens Advice Bureau (CAB)

Call 0800 144 8848 or visit www.citizensadvice.org.uk

Companies House

Visit www.gov.uk/government/organisations/companies-house

Crimestoppers

Call Crimestoppers on 0800 555 111 or visit www.crimestoppers-uk.org

Cyber Aware

Visit www.cyberaware.gov.uk

Financial Conduct Authority (FCA)

Call 0800 111 6768 or visit www.fca.org.uk

Friends Against scams

Visit www.friendsagainstscams.org.uk

Get Safe Online

Visit www.getsafeonline.org

Have I Been Pwned

Visit www.haveibeenpwned.com

Mail Preference Service

Call 020 7291 3310 or visit www.mpsonline.org.uk

National Cybersecurity Alliance

Visit www.staysafeonline.org

National Cyber Security Centre

Visit www.ncsc.gov.uk

Online Dating association (ODA)

Visit www.datingagencyassociation.org.uk

Refuge

Visit www.refuge.org.uk/

Think Jessica

Visit www.thinkjessica.com

Trading Standards

Call 0808 223 1133 or visit www.lincolnshire.gov.uk/trading-standards-consumers

UK Finance

Visit www.ukfinance.org.uk

Victim Support

Call 0333 3007150 or visit www.victimsupport.org.uk

Recovering Monies

First and foremost, decisions to refund any monies is down entirely to the bank or other financial institution concerned. Action Fraud or police have no part in the decision-making process conducted by banks or other financial institutions.

You must also be aware that fraudsters may pose as companies that can recover your money for an upfront fee. This is another type of fraud called **'Recovery Fraud'**.

CONSIDER THESE AND CHECK THEM OUT ONLINE:

Which? (www.which.co.uk) has advice about what to do if you're the victim of a bank transfer fraud (also known as an authorised push payment APP). Generally this will require you to complete a form to send to your bank detailing the circumstances of the APP. National Trading Standards have a reimbursement toolkit on their Friends Against Scams (www.friendsagainstscams.org.uk) website in their **'Where to get help'** section.

Have a look at **Section 75 of the Consumer Credit Act** if you made your payment using a credit card for purchases over £100 but less than £30,000.

Whilst debit card transactions aren't covered under Section 75 of the Consumer Credit Act, you could check to see if you can claim a refund under a voluntary scheme called '**Chargeback**'.

You can check any payments made on online payment platforms such as **PayPal, Apple Pay** or **Google Pay** and see if you can make a claim under the dispute resolution process. You will have to consider any of their Terms and Conditions that might apply.

Online marketplace purchases may be covered under **buyer protection schemes** so check them out. It's a good idea to have a look at how you will be covered before you make a purchase.

Making Reports

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

If you think you've received a phishing email, you can report this to; www.ncsc.gov.uk NCSC stands for the National Cyber Security Centre.

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

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.

REMEMBER, IF YOU'RE NOT EXPECTING IT, ALWAYS QUESTION IT!