
THE LITTLE BOOK OF
FRAUD
STOP!
THINK FRAUD
NATIONAL CAMPAIGN AGAINST FRAUD
POLICE
SCOTLAND
Keeping people safe
POILEAS ALBA



Andy Patrick
Detective Chief Superintendent
Head of Cyber and Fraud Unit

Police Scotland is pleased to introduce The Little Book of Fraud reproduced with the kind permission of the Metropolitan Police Service. This booklet is to help people recognise fraud at an early stage, protect themselves, their families and communities and know what to do if something goes wrong.

Fraud is one of the most common crimes in Scotland and among the most challenging to tackle. It is largely driven by the rapid growth of online fraud and computer misuse, with criminals continually adapting their methods to target individuals and organisations.

Fraud does not discriminate. It can affect people of all ages, backgrounds, and professions. Criminals often exploit human traits like trust, urgency, fear, and curiosity. The impact of fraud can extend beyond financial loss, with victims experiencing significant emotional and psychological harm.

This booklet aims to help people understand how fraud works, how criminals operate, and, importantly, the steps everyone can take to reduce their risk of becoming a victim. It covers a wide range of modern fraud types including investment, romance, impersonation and online shopping frauds, and financial exploitation, reflecting the realities people face today.

Prevention is key to addressing fraud. I hope the information in this booklet provides you with the confidence and knowledge to recognise the warning signs of fraud, make informed decisions and stay safe.

Tackling fraud is a key priority for Police Scotland. If you think you have been a victim of fraud, I encourage you to report it to Police Scotland.



Martin Lewis

We are all potential scam and fraud victims, including me. Don't be under any illusion that it's only those who 'don't get it' who fall for scams. Scammers can be organised, savvy criminals. They are hugely adept psychologically, with the skills to draw people in and steal money and data.

The Met's 'Little Book of Fraud' is intended to tool you up on how to spot potential problems and how to slow a conversation down if you are being asked to send money. And if you do, or have, fallen foul of a scam, this booklet has guidance on what to do next.

Sadly, scams have become a big part of my life. The data shows my face is the one most used by scammers in the UK (what a terrible back-handed compliment!). Their aim is to deliberately pervert my work helping consumers to maximise what they can steal. I've had ads showing me having been beaten up, arrested and more. Anything to tempt you to click. So be aware these criminals will do anything, use anything, to try and get your money.

Worse, scams don't just impact people's bank balances. I've heard from too many people who have had their lives devastated by it. It can lead to a loss of self-esteem, guilt, anxiety and depression. It shouldn't – the scammers are the wrong-doers – but it does.

Initiatives like this one are important. Yet online, at least, it is still an unregulated wild-west and you have to protect yourself. We succeeded in getting scam ads into the Online Safety Act, but it won't be implemented for years, and even then, many outlets aren't covered. So ensure you understand scams, be sceptical, and treble-check before giving people your money.

Contents

4 Introduction
5 Social Engineering
7 Online Crime
11 Artificial Intelligence and Fraud

13 Types of Fraud
13 Romance Fraud
18 Investment Fraud
22 Courier and Impersonation Fraud
25 Advance Fee Fraud
27 Postal Fraud
29 Banking and Card Fraud
31 Payment Diversion
32 Tech Support Fraud
34 Identity Fraud
36 Online Purchase Fraud
39 Financial Exploitation

41 Further Advice
47 Reporting Fraud

Introduction

Police Scotland are supporting the UK Government's National Campaign Against Fraud.

STOP! THINK FRAUD
NATIONAL CAMPAIGN AGAINST FRAUD

Stop! Think Fraud is the national campaign against fraud and has been developed by the Home Office, National Crime Agency (NCA), National Cyber Security Centre (NCSC) and in consultation with a wide range of other partners and external stakeholders.

It supports the delivery of the Fraud Strategy with a multi-channelled campaign aiming to increase the likelihood that people will take action and adopt behaviours that will prevent them becoming victim to fraud.

Fraudsters aren't fussy. They'll pick on anyone.

Nobody is immune from fraud. The criminals behind it target people online and in their homes, often emotionally manipulating their victims before they steal money or personal data.

But there is something we can do. By staying vigilant and always taking a moment to stop, think and check whenever we're approached, we can help to protect ourselves and each other from fraud.

Find out more at gov.uk/stopthinkfraud

Social Engineering

Criminals committing fraud will try to trigger an emotional response in us through creating anger, fear, concern, fear of missing out, shame, love, helpfulness or curiosity; pretending to be people we trust, reputable businesses, potential love interests, experts and charities to get us to act quickly. They add time pressure to make us react to the emotional response instead of stopping to think.

Fraud occurs when criminals deceive you for financial gain. All the types of fraud described in this booklet involve lies or some sort of misrepresentation.

Criminals are incredibly persuasive and use techniques to make us feel at ease. The language used is skilfully designed to abuse vulnerabilities, undermine people's confidence and manipulate decision-making in a similar way to domestic abuse and psychological grooming.

It will make requests seem reasonable and expected instead of a cause for concern. Criminals seek out and isolate victims who may not even realise that they are being targeted.

Social engineering is the practice of using deception to manipulate us into performing actions or providing sensitive information. Social engineering attacks, where trust is abused to gain information, can happen both online and offline. Some attacks, such as phishing, target large groups of people but others target individuals.

In some instances, criminals use data leaks and hacks to find out personal information about us, including our previously used usernames or passwords to help build our trust. They might also pretend to be from a government department or a reputable organisation to establish credibility.

Criminals combine social engineering with time pressure to **make you act quickly without thinking**. This pressure may be obvious or implied. For example, they might say *"If you don't do this in the next 5 minutes, you will lose out on a good offer"* or *"A new payee has just been added to your account"*; making you worry that if you don't act quickly you will lose money.

Criminals also use **current events or times of year** to make the fraud potentially more relevant to you, such as sending out parcel text messages in the lead up to the festive season.

Anyone can be the victim of fraud.

How to protect yourself

- **Knowledge is your best defence.**
- **Legitimate professionals will never rush you** into a decision. If you feel uncertain or pressured, give yourself time and don't hesitate to say "No."
- **Request more time** to check someone is legitimate before speaking to them. If the person is genuine, they will understand. If they become pushy or insistent – end the conversation and walk away.

Stop, Think Fraud.





Online Crime

The internet has become an important part of daily life – we shop, bank, and socialise online. Unfortunately, criminals also use the internet to find victims. The majority of fraud now involves some use of computers or phone communication.

Fraudsters take advantage of the anonymity and global reach of the internet to deceive, hack and steal. They might send emails containing malicious software, create fake websites that pretend to be real businesses, or probe for weak passwords to access your data.

Phishing is a type of online crime where an individual is persuaded into sharing personal information or data by a criminal pretending to be from a trustworthy place. This type of crime is commonly committed via emails (phishing), text messages (smishing) or QR codes (quishing). Messages contain links to fraudulent sites or applications which are designed to look like real websites.

They often pretend to be services that everyone uses such as banks or delivery companies so that they have common appeal. Phishing attacks are normally high-volume, mass communications which are sent to lots of people.

Spear-phishing is a type of phishing where a criminal will target a specific person. Often they pretend to be someone you would trust with financial transactions or security. Criminals use information from data breaches to help them create trust or credibility.

Spoofing is the process of criminals disguising themselves to look as though they're a known or trusted source.

How to protect yourself

Staying safe online is essential to reducing personal fraud risks and protecting your data from being stolen.

- **Be mindful of what personal information you share about yourself on social media** and other websites. Adjust your privacy settings so strangers can't easily gather information about you and restrict profiles where personally identifiable information (PII) is being shared with individuals you know and trust.
- **Use strong, long and unique passwords** for your accounts. If criminals gain access to your emails, they can reset passwords for other accounts. You can use a password manager to help you remember them; major operating systems typically have these included.
- **Enable two-step verification** (2SV) or biometric and facial recognition on your accounts. This adds an extra verification step to keep out attackers. Further information is available on the National Cyber Security Centre website http://ncsc.gov.uk/cyberaware/home
- **Avoid using public or unsecured Wi-Fi** for sensitive activities like online banking.
- **Always lock your devices** with a password, PIN, or biometric identification.
- **Check to see if your email address or password has been leaked** in a previous data breach on http://haveibeenpwned.com
- **Review the permissions and privacy settings** for what data you are sharing with companies. Consider whether the information is necessary for the application or website to function and if it isn't, restrict access to your data.

- **Contact companies by using details found following research** on search engines rather than those provided in the communication. Criminals often include a reputable company name in the email address they use to contact you to make it appear genuine or spoof (imitate) phone numbers.

  Be wary of emails sent to you from free email address providers, for example; Amazon@gmail.com or domain variations such as admin@amazon-support.com

- **Be wary of 'typosquatting'** which takes advantage of common typos people make while using the internet.

  Some criminals attempt to make their sites appear genuine by using subtle differences in URLs such as replacing the case of letters or using a different domain extension; for example using a zero instead of an 'o'.

  This is purposefully not obvious to avoid detection.

This technique is often used for emails, phone calls, websites or IP addresses to help convince you that the contact originates from somewhere that it doesn't.

Some criminals will use phishing attacks to get through spam filters by putting malicious content in attachments.

Because of this, avoid clicking on unknown attachments.



Precautions & Protection

Criminals target you in crowded areas such as on public transport, bars, shops or cafes, or when at a state of heightened vulnerability such as when intoxicated.

They may watch or film as you input private information such as passwords or security patterns. It is common for mobile phones to then be stolen.

Criminals can then quickly change the necessary passwords or security features to move funds from bank accounts and digital wallets, or make purchases on applications.

- **Be aware of surroundings** when accessing your device, particularly when entering your PIN numbers or passcodes.
- Ensure your phone's **anti-theft features** are switched on.
- **Hide applications** such as banking applications or digital wallets in secure folders or consider whether they need to be on your phone at all.



Artificial Intelligence and Fraud

Advances in Artificial Intelligence (AI) have created new tools that criminals can abuse to commit fraud. Modern AI systems – especially "generative AI", which can produce text, images, or voices – make it easier to create highly convincing fake content.

For example, a fraudster might use AI to generate emails or messages that sound exactly like a real person, or even to clone a person's voice from a short sample. This means a criminal could impersonate someone you trust or craft believable fraud messages on a large scale.

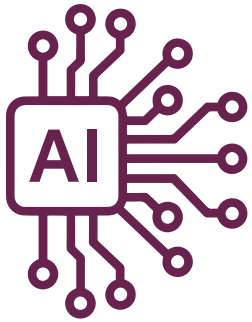
How to protect yourself:

Be aware of the potential for AI-driven fraud:

- Remember that **criminals may use AI to enhance their communication**. If you receive an unexpected call from a family member or friend that seems unusual or asks for money, be cautious – it could be an AI-generated voice.
- Always **verify claims through a secondary method** like calling back on a known number.
- **Double-check information** that you see online, even if it looks professional or authoritative. AI-generated text or deepfake media often looks real. Cross-reference claims or requests with a trusted source. For instance, if you see a video message from a friend or celebrity that doesn't sound like them – consider that it might be synthetic. Verify through direct contact with the person or another reliable channel before acting.



- **Check an independent platform** before signing up for promotions to confirm the legitimacy of what is being offered.
- Social media platforms use authentication marks to signify trust. Fraudsters, however, are known to have purchased or falsified 'blue ticks' to appear legitimate. **Cross-reference account names, even those with authentication marks, against official sites** or independent platforms to make sure that you're viewing genuine accounts instead of near-identical copies.
- Be careful about using new AI-based tools or browser extensions that ask for access to your accounts or personal data. **Research their credibility** and security. Malicious software can be disguised as helpful AI assistants.



Types of Fraud

Romance Fraud

The way in which we meet people for relationships has changed. Finding love or companionship on dating websites and apps has become common. Romance fraud happens when people are tricked into false relationships by criminals who aim to steal their identities or money. Criminals are well practised at building trust and manipulating people so that when money is asked for, this doesn't seem unreasonable.

Romance fraud can have a severe financial, social and emotional impact upon victims and is similar to grooming, domestic abuse and coercive control. This type of crime may be identified by family and friends first as victims may feel they are making decisions which are rational and reasonable. This, and a sense of embarrassment, can have a negative impact on willingness to report what's happened.

The following are common tactics used by romance fraudsters to manipulate you:

- **Setting up the relationship in a harmless and expected way** by providing information about their life, job, family, aspirations and wishes.
- **Verifying their existence by introducing other criminals** who pose as family members, friends or professionals to make their story seem convincing.
- **Distracting you with promises** for the future.
- **Disguising requests for money**, requesting it in an indirect way or suggesting that the need for financial support is temporary. This can come from the drip feeding of information so that when asked for, it doesn't raise concern. They may also make you feel it's your idea or initially turn down your offers for financial assistance to build your trust.

- **Encouraging secrecy**, cutting you off from your support networks and making you feel disloyal for seeking advice or questioning what is being asked. This is made to seem as if it is mutually agreed rather than a cause for alarm.
- **Manipulating the sense of power** so that you apologise or feel guilty for raising concern, even when this is reasonable, or by the criminal claiming the lack of belief is causing physical or emotional pain.

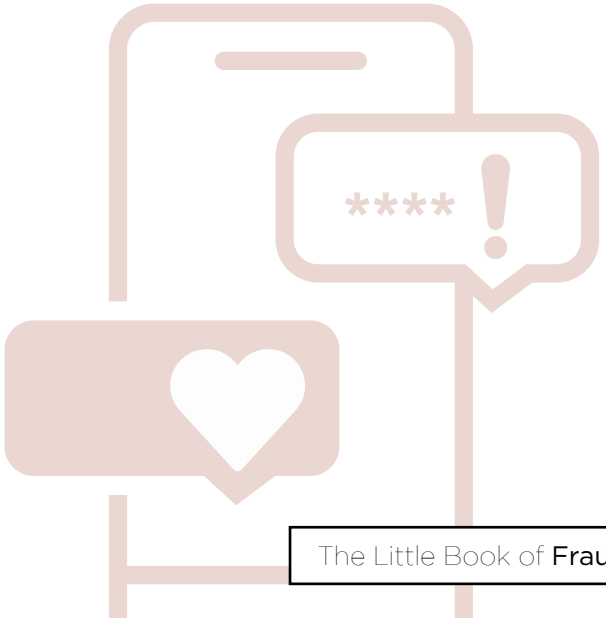
Sexually motivated extortion and intimate image abuse

Sexually motivated extortion is a form of blackmail which involves threatening to publish sexual information, photographs or videos to extort money or to get you to do something against your will. Photographs or recordings are sometimes made without you realising or consenting. Criminals will demand a payment for these videos not to be released.

A criminal may send you nude images, possibly stolen or AI generated, encouraging you to reciprocate, or push for a video call of an intimate nature. Often the demands made are ongoing, not a one-time payment.

These types of crimes are also sometimes committed by individuals who do not hold any such videos of you. They can be committed as part of a phishing attack to numerous people or directed towards specific individuals. The communications from the criminal may also include a password or username from one of your online accounts which has been taken from a data breach to attempt to appear more credible.

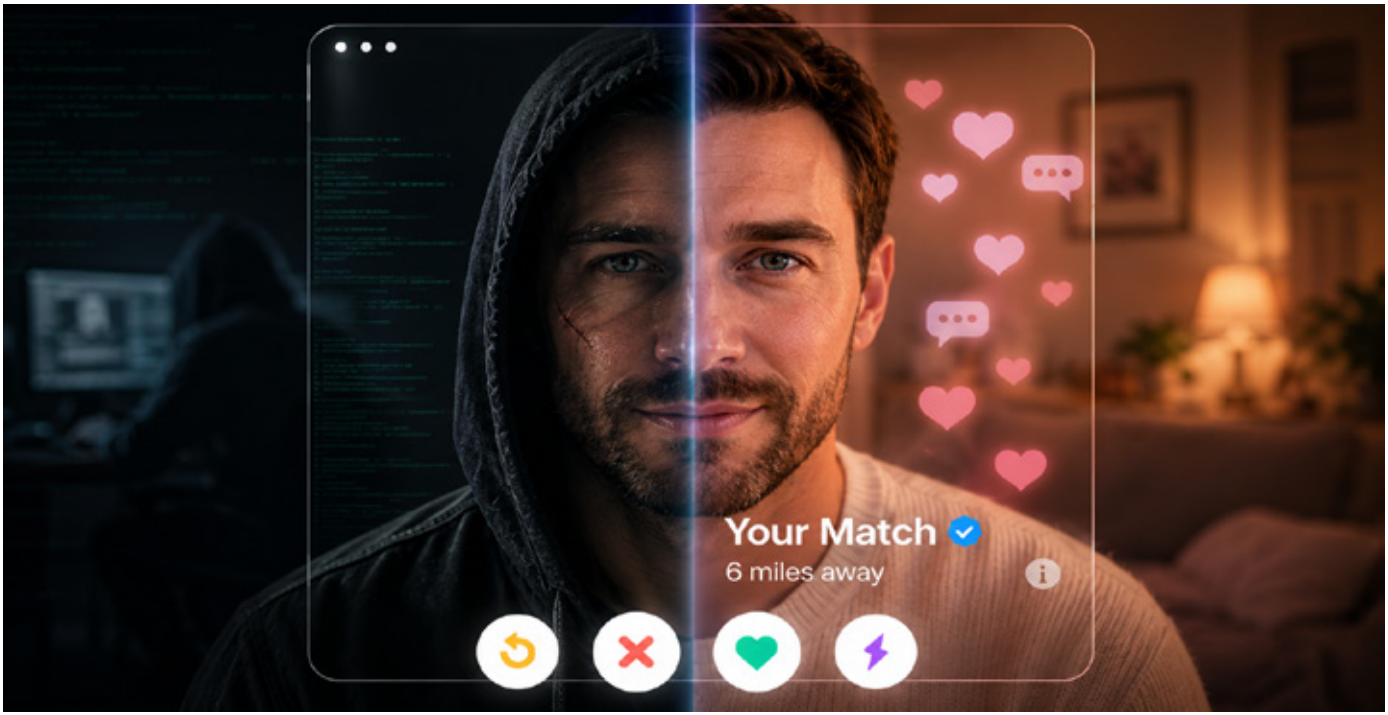
Criminals often target people via social media or dating apps. They rely on the victim being too embarrassed to seek help once threatened. Many victims feel trapped and alone in these situations.



Socially engineered investment fraud

Fraudsters will sometimes combine fraud types, such as initially starting a relationship but then suggesting that they can help you with investments. This can be through any trust-based, false relationship which may be romantic, friendship or through someone posing in a professional capacity.

Having contacted you online, they build rapport over a period of time before bringing up the success they've had with a great investment opportunity and encouraging you to get involved. By the time that money is requested or investment encouraged, you will have been primed to believe that this is legitimate so the request may not feel unexpected. It is common for intelligent and tech-savvy individuals to be targeted.



Because you've grown to trust them, you're more likely to believe the investment opportunity is real. They may claim to be successful with their work or live a lavish lifestyle which suggests they have invested well themselves or have the funds to pay you back. They may also pretend to be investing along with you. Just like in investment fraud (see page 18), the criminal's primary focus is to get you to part with money or personal information.

Be aware that the contact may not necessarily be on a dating site – they could begin the contact via social media messages or a text message they pretend was meant for someone else. This type of fraud is likely to have a high emotional impact.

Remember that **not everyone is who they claim to be**.

How to protect yourself:

- **Be aware of what personal information you are providing** about yourself online and **never provide copies of your personal documents** to anyone you haven't met including passports or driving licences.
- **Block and report profiles** to social media platforms from individuals who create a sense of obligation to respond.
- Criminals will often try to move the conversation to an **encrypted application**. This makes it harder for law enforcement to gather evidence and trace the individual.
- **Don't send any money or crypto to people you haven't met**, regardless of how long you've been speaking to them or how much you trust them. Avoid transferring money on their behalf, taking out loans for them, sending or receiving parcels for them, or allowing them access to your bank accounts.

- **Perform a Reverse Image Search** for pictures which may have been taken from somewhere else – for example through https://www.tineye.com. Examine the metadata of images provided to determine if these are generated by Artificial Intelligence. Be wary of videos where there is a mismatch between audio and motion, or distortions in mouth movement.
- If in doubt, **ask your friends and family** to sense-check the situation. It may be difficult to judge someone if you are too close. Be wary of anyone who is encouraging you to keep information away from your support network.
- **Be cautious of unsolicited messages** on social media platforms or dating applications as well as 'wrong number' texts and contact through group chats.
- If you're engaging in intimate communications with a new online acquaintance, it's safer to **avoid doing anything on video that you wouldn't want shared publicly**.
- In the case of sextortion, **do not panic**. Non-judgemental help is available.
- **Do not pay the money** which is being requested. Many victims who pay continue to get demands for higher amounts of money. In some cases, even when demands are met, the criminals will still post the videos online.
- **Save all evidence** of the interactions (messages, screenshots, etc.) and contact the Police.



Investment Fraud

Investing in stocks, shares and commodities can be a successful way of making money, however it can also lead to people losing their whole life's savings. Criminals will try to persuade you to invest in schemes which are fake, non-existent or aren't worth the money that was paid.

Within the UK, there are a lot of investment frauds; both with traditional investments but also with emerging technology such as crypto. Criminals will offer you high rates of return, particularly over longer periods of time, which often do not exist.

Criminals may direct you to well-presented websites or send you glossy marketing material. These resources do not mean they are a genuine company. Many fraudulent companies have a polished customer image to cover their illegal activities.

'Experts' may showcase the huge profits they say they have made through their investments and offer to teach you to do the same or offer to do this on your behalf. This will often use tactics to make you act quickly; even if you feel that you are in control.

Often, initial investments will yield small returns as an incentive to invest further. 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 promised returns lost.



Often, criminals target people who have some savings or have been involved in previous investments, or those who've been defrauded before. Common types of investment fraud include:

- **Ponzi/pyramid schemes:** You're invited to invest in a venture and bring in other people to invest too. The more people you on-board, the better the returns. Early investors might receive some returns, which are really just funds from newer investors. This illusion of success draws in more money and people until the scheme collapses.
- **Boiler room stock fraud:** High-pressure salespeople call to sell shares in a company that they say is about to dramatically increase in value. They often have glossy brochures and websites to back up their story. In reality, the shares are worthless and, once you buy, the criminals disappear, or the shares become unsellable.
- **Cryptocurrency fraud:** Crypto-assets, also commonly referred to as 'cryptocurrency', 'tokens' or 'coins', are digital representations of value or rights which can be stored, transferred and traded.

  They are so called as they use cryptography to secure communications. There are thousands of coins currently in existence including Bitcoin, Ethereum and Ripple.

  Crypto-assets tend to be volatile, speculative and their use comes with a number of risks. Within the UK, although certain laws and regulations apply to them, they are not regulated as strictly as banks or the stock market and losses are unlikely to be covered by the Financial Services Compensation Scheme (FSCS) so you may struggle to get your money back if your assets are lost; even to fraud.
- **Land banking or rare commodity fraud:** You're offered to invest in something such as land, gold mines, rare earth metals, exclusive art or whisky collections. The product is often real in concept but misrepresented in value. You pay money for something that either doesn't exist or is nearly worthless and impossible to resell.

The criminals who run these schemes are often very convincing. They may have professional-looking websites, fake testimonials and official registration numbers. Some register a UK company to appear legitimate, or use a prestigious virtual office address (such as London's Canary Wharf or Mayfair) to appear well-established. They exploit the fact that most people won't visit these addresses.

They commonly use tactics such as:

- **Telling you that this is a limited-time offer**, encouraging you not to miss out.
- **Name-dropping authorities** or claiming celebrity endorsements.
- **Advertising via a sophisticated website** where you register interest and they subsequently contact you to follow up. They then give you personal attention and refer to "investment analysts" who answer your questions whilst encouraging you to invest.

Another danger is **recovery fraud** targeting past investment fraud victims. If you've lost money from a fraud, you might later be contacted by someone claiming to be from a law firm or investigative agency who can help recover your funds. They will charge fees to recover your money. This is a secondary type of fraud used to get further money from you.

How to protect yourself:

- Thoroughly **research all products and companies** and **seek advice** from a regulated, independent financial advisor prior to investing.
- **Read reviews** to determine whether the team behind the business hold the relevant experience and whether they are backed by credible venture capital or strategic advisors.
- **Check if a firm or individual is registered** with the Financial Conduct Authority using their Firm Checker – https://www.fca.org.uk/consumers/fca-firm-checker. If they are not listed, treat contact with caution. Add search terms such as 'fraud' or 'scam' alongside the company name to review other people's experiences.
- Even if a firm is on the FCA register, **be wary of "clone firms."** These are schemes where fraudsters use the name, address, and registration number of a real business to appear genuine.

Always use the contact information provided on the official FCA website, not what is provided to you, to get in touch with them and verify any communication you have received.

- **Use the FCA's Investment Checker** to check any investments you have been offered https://www.fca.org.uk/scamsmart. Secretive or complex strategies can be used to disguise fraudulent schemes so be wary of excuses for why you can't review information about investments in writing.
- **Be sceptical of time-limited offers or pressure** to act now. Criminals push you to act before you have time to think or seek advice.
- **Ignore 'Low risk, High reward' advertising** – every investment carries risk. Even genuine investments go up and down over time so overly consistent return promises should be treated with caution.
- **Criminals exploit trust** derived from membership of a group who share an affinity through national, ethnic or religious affiliation. Respected or prominent members may be enlisted both knowingly and unknowingly to advertise investments.
- If you have invested and something feels wrong, the communications after payment are inconsistent, or you're asked to pay more fees unexpectedly, **do not send more money**. Pause and investigate further. Fraudsters often ask for more once they sense a victim has invested too much to walk away.
- If you believe you have been defrauded, **inform your bank and make a report to Police Scotland** as soon as possible. In some cases, if you act quickly, there's a chance to freeze transactions or retrieve lost funds.

Courier and Impersonation Fraud

Criminals may pose as officials from a bank, the police, HMRC or another trusted authority to deceive you into handing over money or personal information.

These fraudsters typically contact you by phone, text or email, claiming there's an urgent problem: for example, there has been suspicious activity on your bank account, your credit card was used fraudulently, or they're investigating a crime and need your help. They may tell you a business such as a currency exchange, bank or jewellers is operating fraudulently. They then ask you to take specific actions which ultimately lead to you parting with your money or high value items. Examples of this include:

- **Withdrawing a large sum of cash** from your bank account and handing it to a courier or someone impersonating a police officer who will come to your door.
- **Purchasing high-value items or gift cards**, then giving them to a person sent to collect them.
- **Transferring your money into a new "safe account"** because your current account has been "compromised". The account information you're provided will be linked to the criminals.
- **Handing over your bank cards and PIN.** Criminals arrange for a courier to pick up your card or exchange it for a new one. Criminals often provide false verification codes or ask you to input your PIN number to confirm your identity. This is to encourage you to say or enter your PIN where they can capture it. With your card and PIN, the criminals can spend your money.



Throughout these types of fraud, the criminals usually insist that you keep things secret; telling you that bank staff or other authorities are involved in the supposed crime. This prevents you from speaking to the professionals who are trained to protect you.

Doorstep traders: A related form of impersonation happens face-to-face, when criminals come directly to your door. These individuals might pose as tradespeople, utility company representatives, professionals or charity workers. They often offer services you haven't asked for such as fixing a loose roof tile, testing your water purity or charity fundraising. In reality, they intend to defraud you. A builder might convince you that your house needs urgent repairs, then charge you much more than is reasonable for little or no work. They frequently ask for cash up-front and pressure you to act quickly. In some cases, they may distract you so that they can enter and steal items from your house – sometimes with one person speaking to you at the door while another steals your valuables.

How to protect yourself:

The police, your bank or any other trusted organisation will:

- **Never** contact you to withdraw cash or transfer money
- **Never** ask you to purchase or send cash, foreign currency, jewellery, gold bullion, crypto or other items
- **Never** ask a courier to collect items or for you to post cash or other expensive goods
- **Never** ask you to help in an investigation
- **Never** call to ask you to verify your personal details, banking information or PIN by phone or offer to pick up your card or PIN by courier

Hang up if you get a call like this.
If you are told to call another number immediately to verify the person on the phone, hang up the phone and wait five minutes before using the same phone line; fraudsters may stay on the line after you hang up. Alternatively, use a different line altogether to call your bank or the police.

- Contact your bank from the number on the back of your card or **159** rather than any numbers given to you
- **Your debit or credit card is yours** – don't let a stranger take it off you
- **Speak to friends or family before taking action.** Alternatively call **101** for non-emergency incidents. Always call **999** in an emergency
- If someone comes to your door claiming to be from a trusted company, always **check their identification thoroughly**. If you're not sure about who they say they are, refuse entry and call the company they claim to represent to verify if they are legitimate. A genuine worker will not object if you take these precautions. Never leave your front door open and unattended.
- **Never agree to have work done on the spot** by someone who knocks on your door out of the blue. If they say you have a problem, seek out a second opinion. Be wary of phrases such as "urgent" or "special deal – short time only."
- If you feel threatened or alarmed by a doorstep caller, **close the door and call a trusted person for help**.

- If you realise you've been the victim of a courier or impersonation fraud, **contact your bank immediately**. Explain what has happened. Banks can sometimes freeze accounts or undo transfers if alerted straight away. Also report to Police Scotland (see last page of this booklet).



Advance Fee Fraud

"Advance fee" fraud is where a criminal convinces you to make upfront payments for goods, services or rewards that never actually materialise. This could be a prize, loan, inheritance or an item at a bargain price. Once you pay, they either disappear or come up with reasons you need to send more money.

Common examples of advance fee fraud include:

Recovery Fraud

After you've already been a victim of fraud, the criminal contacts you claiming they can recover your losses for a fee.

Inheritance Fraud

You're told you're in line to receive a large inheritance, but you must pay a fee to release the funds.

Lottery Fraud

You're told you've won a prize but must pay an admin fee to claim it.

Loan Fraud

You're asked to pay an upfront fee for a loan.

Racing Tip Fraud

The criminal offers "guaranteed" winning racing tips for a fee.

Rental Fraud

You pay an upfront fee to rent a property that doesn't belong to the person advertising it or doesn't exist.

Work-from-Home Fraud

You're offered "easy money" for working from home, but must pay for leads, a kit or a website first.

Cheque Overpayment Fraud

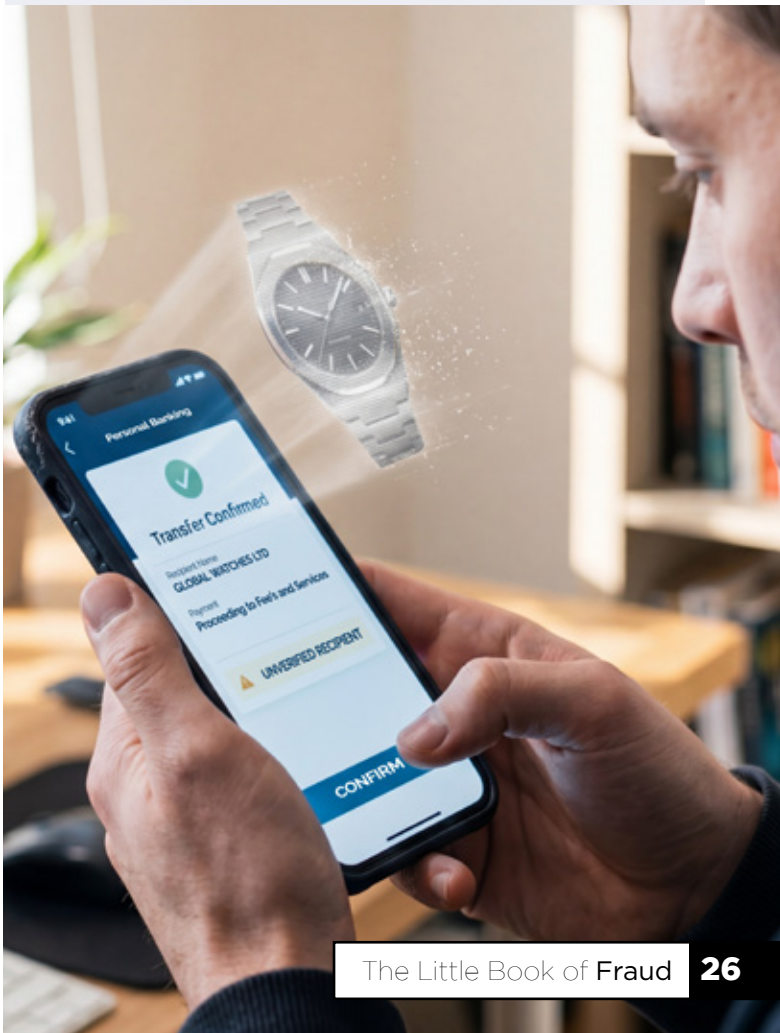
The criminal overpays for something with an invalid cheque and asks for the difference back.

Matching Fraud

After you place an advert to sell something online, often vehicles, the criminal charges a "refundable" fee to connect you to a non-existent buyer.

How to protect yourself:

- **Be sceptical of any unsolicited communication** that promises a large benefit (money, prize, etc.) in exchange for upfront fees or payments. Ask yourself: *Why would I need to pay money to receive a gift or winnings?*
- Remember that **if you didn't enter a lottery or competition, you cannot win it**. Any message that says otherwise is a lie.
- Sometimes genuine authorised firms will ask you to pay an upfront fee before they provide a loan. If they do, they must **send you a notice** setting out specific information. You will then need to reply to the notice saying you understand and agree with what it says. Further information about loan fraud is available on the FCA website; https://www.fca.org.uk/consumers/loan-fee-fraud
- **Independently verify the company or individual** by finding your own contact information for them – do not use phone numbers or email addresses they have sent you, or click on links, as they likely belong to the criminals.
- **Never be rushed** into paying. Advance Fee fraudsters add time pressure to make you act quickly. Take your time and consult with someone you trust before sending any money.
- If you have already paid an upfront fee and the other party **keeps asking for more**, stop. Cut off communication and do not send additional funds.



Postal Fraud

Not all fraud happens online or by phone – many attempts to defraud us still arrive through the post. So-called "scam mail" refers to letters sent in bulk to people's homes, often claiming that the recipient has won a prize or can claim a large sum of money. Typically, the letter asks you to send a fee, make a purchase or provide personal details in order to receive the winnings or reward. In reality, there is no prize; criminals are simply collecting money (and information) from as many respondents as possible. Fraudulent letters take many forms:

- **Fake lottery and prize notifications:** You receive an official-looking letter saying you've won a big cash prize in an international lottery or sweepstake. It might have fancy seals or stamps. The catch is you need to send a "processing fee" or "tax" (often relatively small) to release your winnings.
- **Fake business related post:** If you're a business owner, a letter may arrive from, "Companies House" or "HMRC" asking you to send a processing fee in order to complete your company registration.
- **Fraudulent charity appeals:** You might get post from a charity raffle or a contest where every ticket is a winner; claiming you have to send money to receive your prize. The charity might be fake or, if it's real, the contest is not authorised by them.
- **Inheritance and investment letters:** Like emails, some letters claim that a rich person has died and you are in line to inherit, or they offer a too-good-to-be-true investment. They request upfront fees or personal data in exchange for the payment.

How to protect yourself:

- **View any unexpected prize or offer of money with scepticism.** If you have truly won a lottery or prize, you will not be asked to pay an upfront fee to receive it.
- **Guard your personal information.** Some fraudulent post will ask for a lot of personal details. Providing these can lead to identity theft or more personalised fraud. Don't fill out forms provided from unsolicited offers.
- If you or a family member receive post that promises fortunes or plays on emotions, **discuss it with someone you trust**.
- **Opt-out of junk mail** by registering with the **Mail Preference Service (MPS)** to reduce unsolicited marketing. While this won't catch all fraud (especially that coming from overseas), it can reduce the amount your address is visible on marketing lists.
- **Report fraudulent post.** Royal Mail has a service to handle fraudulent post – you can forward the letters to **Freepost Scam Mail** or email reportascam@royalmail.com. They can investigate and can arrange to intercept further letters.
- When in doubt, **throw it out**. It's better to lose the chance at a prize than to risk losing money to fraud. Shred letters that contain personal details so criminals can't harvest information from your bins.



Banking and Card Fraud

Criminals have many tactics for stealing bank account details, payment cards or cash from individuals. Some involve technology, while others use social engineering techniques or physical theft. Here are some common methods:

- **Cash machine (ATM) fraud:** Criminals tamper with ATMs by attaching skimming devices that capture card data, or tiny cameras that record you entering your PIN. They might also engage in "shoulder surfing" (watching over your shoulder) or distraction theft, where one person distracts you with conversation and, when you're distracted, an accomplice takes your card or money from the ATM. In other cases, an ATM may retain your card because a device was installed. Criminals will then wait until you leave to retrieve the card.
- **Card theft and cloning:** Your physical bank cards are targets too. Thieves can steal cards from wallets or intercept new cards in the mail. When you hand your card for payment to a retailer, if it's taken out of sight, it could be run through a skimmer (illegal card reader) to copy data. Contactless cards have certain protections including a limit on contactless transactions but if someone steals your card and PIN number, they can still make higher numbers of purchases before the card is reported as missing.
- **Online banking and payment fraud:** Instead of persuading you to transfer money, some criminals try to break into your account directly. They may use emails or texts that look like they are from your bank, asking you to click on a link to verify details. That link may lead to a fake website that records your login information. Clicking on fake links or opening attachments may install malicious software on your computer or phone which can also log your keystrokes or give a criminal remote access to your online banking. If they get in, they can attempt to transfer money or harvest personal data for identity theft.

How to protect yourself:

- **Be vigilant at ATMs.** Don't use it if anything looks unusual. This could include loose parts or fixtures over the card slot or keypad. Shield your PIN with your hand whenever you enter it. If someone tries to distract you or gets too close, cancel the transaction and retrieve your card. If your card is stuck in an ATM and a stranger offers assistance, decline. Instead, contact your bank as soon as possible to report the incident and cancel the card.
- **Keep payment cards secure.** Carry cards in a Radio Frequency Identification (RFID) wallet. This blocks electromagnetic signals and protects cards from skimming/scanning. If a card is lost or stolen, report it to your bank immediately so it can be blocked. Quick reporting can prevent fraudulent transactions.
- When making a card payment in a store or restaurant, **watch what happens with your card**. If the staff need to take your card away, consider accompanying them or ask if a portable card reader is available. It's your right to protect your card data.
- **Review your bank and credit card statements often.** Look for any transactions you don't recognise, no matter how small. If you see something strange, notify your bank right away.
- For online banking, always go to your bank's website by typing the address yourself or using a bookmark you trust. **Don't log in via links sent in emails or texts.** Similarly, be cautious with any email or message that asks you to "verify" account details or passwords.
- **Use strong, unique passwords** for your financial accounts. If your bank offers two-step authentication, enable it.
- Keep your computer and smartphone secure. **Install reputable security software** including anti-virus protection and keep this updated. Avoid completing banking transactions on public networks.
- Remember that **banks will never contact you by email or phone to ask for your PIN**, password, or to move your money.
- **Don't connect any unknown or untrusted devices** such as USBs into your systems.

Payment Diversion

Payment diversion targets people with the intention of getting them to transfer money to a bank account operated by a criminal. Criminals use spoofed (imitated) sender email addresses which appear to come from a known person.

The rouse that criminals use varies. In some situations, they may claim to be a senior member of staff within a company and will ask the receiver to make a payment or transfer funds for an ongoing or new business transaction. In other situations, they claim to be a solicitor requesting balances for house purchases. Often the payment request is marked as urgent, or pressure is applied to make the payment as soon as possible.

- Criminals target these types of attacks at times of year when people are making lots of payments. They may also research people to understand when large payments are going to be made to target them.
- In these situations, the accounts where funds are sent will be under the control of criminals and any funds paid into them will be lost.
- If an email is received requesting a change of bank details on an account or a one-off payment, verify this by making direct contact with the organisation or person requesting the change. Do not use any contact details provided in the email and don't be pressurised by any email or follow up phone call as this may be the criminal.



Tech Support Fraud

Tech Support Fraud (also known as computer service fraud) occurs when someone pretends to be a technician or customer support representative in order to defraud you. They may phone you saying that your computer has a virus or errors that need fixing urgently. Alternatively, you might see a pop-up on your screen claiming your computer is infected and telling you to call a number for help.

These criminals often ask you to install a remote access program so they can connect to your computer or guide you through various screens on your system to show fake problem indicators. Sometimes they claim that normal system logs are viruses. They will then pressure you into paying for a service or software to "fix" the issue. This could be a one-time payment or a subscription. They might ask for your card details, or request payment via bank transfer or gift cards. In some cases, while they have remote access, they may install malicious software or steal data from your machine.

Another tactic is **refund fraud**, where you receive an unexpected email or call from a company saying you're due a refund for a service such as an overpaid subscription or an unrenewed service. The criminal then "helps" you receive the refund by asking you to log in to your online banking while they are connected to your computer. They will manipulate what you see on your screen to make it look like they have accidentally refunded you too much money. They then ask for you to send back the difference, often via a quick method like a wire transfer or via cryptocurrency. In reality, there is no actual refund – the money you send goes to them and the "excess money" you thought you saw in your account was just a fake screen.



How to protect yourself:

- Companies will not contact you out of the blue to tell you that your computer has a problem. Any unsolicited tech support call is very likely a fraud. **Hang up straight away**.
- **Do not trust pop-up messages** or emails about your computer being infected. If a phone number or email is provided for "customer support," do not use it. **Check customer support numbers using another source before calling**.
- **Never give control of your computer** to someone you do not know. If you need technical help, initiate the call yourself to a known support line by using the number on an official website or the paperwork that came with a product.
- **Be cautious about giving payment details** to anyone who claims to be tech support. If you feel pressured to pay immediately for a "fix" or "subscription," this is a warning sign. Real tech support services usually charge only when you have brought your device for repair or initiated a service request.
- If you suspect you have been a victim of a tech support fraud, **act quickly**. Disconnect your device from the internet to stop any further intrusion. If you provided credit card or banking information, **contact your bank** to stop or dispute charges.
- **Run a full security scan** on your computer, remove software that has been downloaded and **change any passwords** you may have revealed.
- **Educate family members**, especially those less familiar with technology. Many victims are not tech-savvy, and criminals rely on creating confusion and panic.
- **Make regular backups** of important work and data to a separate device such as a portable hard drive. These backups should be stored offline and in a safe place. This will allow the data to be restored if it is infected.

Identity Fraud

Identity fraud is when a criminal uses your personal information to carry out unauthorised actions. Instead of directly tricking you into a payment, these fraudsters steal personal details such as your name, date of birth, address, financial information or National Insurance number. With enough of your data, they can open bank accounts or credit cards in your name, take out loans or make purchases, leaving you with the bills and damage to your credit history.

Information can be stolen in a variety of ways. Some criminals rummage through bins for discarded bills, statements, or expired IDs ("dumpster diving"). Others might steal your mail to intercept a new credit card or bank statement from your post.

A lot of identity theft happens digitally with hackers breaching companies' databases and selling personal records on the dark web, or fraudsters sending phishing emails to trick you into providing login details or personal information.

Social media can also be a rich source of personal information. If your profile is public and contains personal information such as your birthday, family members, schools attended or pet names, a fraudster can use those details to impersonate you or answer security questions in your name.

The impact of identity fraud can be serious. You might start getting bills for things you didn't buy, or debt collectors might contact you about loans you didn't take out. Your credit report could show accounts you don't recognise. In extreme cases, someone could even use your identity when arrested for a crime, which could result in you appearing in Police databases, warrants issued in your name



How to protect yourself:

- **Secure your personal documents.** Shred or thoroughly tear up any paperwork that has sensitive information (such as financial statements, credit card offers or insurance forms) before throwing them away, or consider going "paperless".
- **Be cautious with sharing your personal details online** and on social media. Don't share personal information including your birthday, your pet's names, your mother's maiden name and your address. These can all be pieces of the puzzle that enable identity fraud. Make sure your profile is only shared with people you know and trust.
- Your email is a gateway to accessing other accounts so **secure it with a strong password and two-step verification**.
- Regularly **monitor your bank accounts and credit reports**. You can get free credit reports or use services from credit reference agencies, such as Experian, Equifax or TransUnion. Look for accounts or searches you don't recognise, as these could be indicators of fraud.
- If you receive unexpected communications such as a bill, statement, or a letter about an account you didn't open, **don't dismiss it**. Contact the company immediately and explain the situation, it may be fraud. Do the same if your regular bills or statements stop arriving.
- **Be wary of unsolicited phone calls, emails or texts** asking for personal data. Banks and government bodies won't make contact unexpectedly to ask for personal details.
- Consider using a **protective registration service** such as CIFAS protective registration if you're concerned about identity fraud. This adds extra verification steps whenever credit is applied for in your name. See page 41.
- **Cancel any lost or stolen credit cards** immediately and inform the issuing agency about lost documents such as passports or driving licences.

Online Purchase Fraud

Buying products or services online, from electronics and cars, to event tickets and holiday bookings is incredibly convenient, but it also opens opportunities for fraud. Online purchase fraud occurs when you pay for something online but the goods or services aren't delivered, or they aren't as advertised. The internet's vast marketplaces, especially on second-hand sites and social media, allow criminals to cast a wide net for potential victims.

Goods and auction fraud: Fraudsters often list items for sale that they don't actually possess. They may post fake adverts on popular marketplaces with prices significantly below the item's value. When you show interest, the criminal might invent a reason to move the deal off the official site; offering a discount if you pay them directly via bank transfer or outside of the platform's payment system. Once money is sent, the seller disappears. In other situations, you might "win" an online auction and make a payment, but the item never arrives. If you unsuccessfully bid on an item, the fraudsters may contact you with a second-chance offer to buy the item.

Holiday and travel fraud: Holiday fraud typically involves fake travel websites, listings or airline tickets. You might find a villa for rent or a holiday package that looks perfect and is cheaper than others. The website might appear professional, with glossy photos and even ABTA or ATOL travel protection scheme logos. These are often fake or stolen from genuine listings. After encouraging you to pay, you might receive a confirmation email but it may not be until you arrive at the destination that you discover the booking doesn't exist.

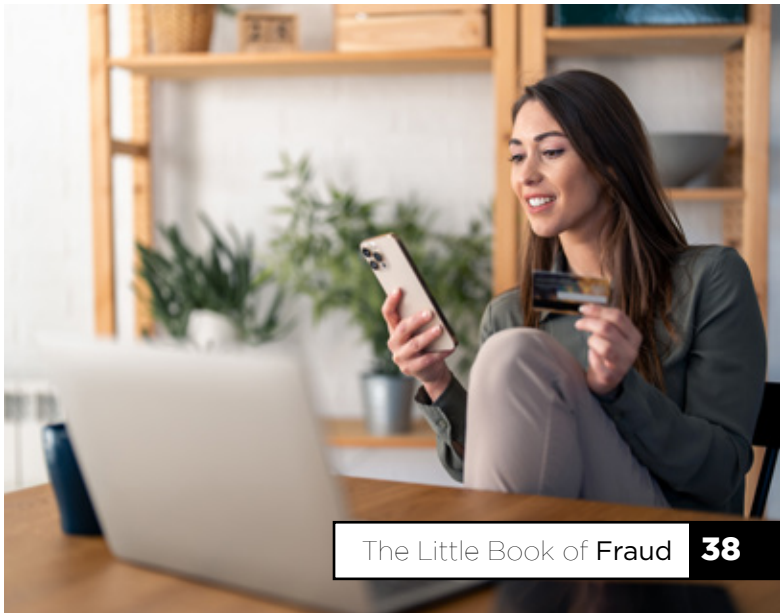
Ticket fraud: When concerts or sports events sell out, fraudsters know people are desperate for tickets. They create legitimate-looking ticket sale websites or advertise on social media. Some will send you what looks like a real e-ticket after payment. Only later do you realise it's been duplicated or forged when you're denied entry at the venue. In other cases, no ticket arrives at all. The fraudster may claim they will meet you outside the venue with the ticket if you just send a deposit upfront. Instead, they take the deposit and do not provide the tickets in return.



How to protect yourself:

- **Always use trusted websites** or official vendors for online purchases. Use consumer websites or reviews from people or organisations that you trust.
- **Do not click in links in emails or texts** that contain promotions which seem unmissable. Criminals can easily duplicate legitimate websites.
- **Use a credit card** when making significant purchases online. Credit cards give you legal protections for purchases between £100 and £30,000 under Section 75 of the Consumer Credit Act 1974, meaning the card company is jointly liable if something goes wrong.
- **Be wary of sellers who push for payment by bank transfer or crypto** as unlike credit cards, these methods are hard to recover money from. Legitimate sellers will usually accept safer payment methods. If someone insists on a bank transfer before delivering an item or ticket, this is a red flag.

- For travel, **use reputable travel agents or booking sites**, and double-check if they are members of industry associations (like ABTA or ATOL for travel). If it's a holiday rental, try to verify that the property actually exists. Read reviews about the seller or the site. If you're on a lesser-known travel site, search online for reviews to see if others have reported problems.
- **Good quality, professional-looking communications are no longer signs of legitimacy.** Criminals can create convincing invoices, emails, or tickets. If you receive a confirmation email, verify it independently using official contact details if you are unsure.
- For event tickets, **buy tickets from the event promoter, venue box office, official agent or a reputable ticket exchange site** or app. If the retailer is a member of the Society of Ticket Agents and Retailers (STAR), you are offered additional protection if something goes wrong. If a website shows their logo, you can check they are really a member on www.star.org.uk
- If a price is dramatically lower than everywhere else, take a moment to consider why. It could be fraud.
- After any online purchase, **keep records of your transaction** (receipts, emails, listing screenshots). If you don't receive the goods or tickets as promised, **report the issue** to the website or platform and **contact your payment provider** as you may be able to get your money back.
- If something feels suspicious about a transaction, the seller is pushy, communication is poor after paying or details don't add up, **act quickly**. Try to halt the payment if possible and report your suspicions.



Financial Exploitation

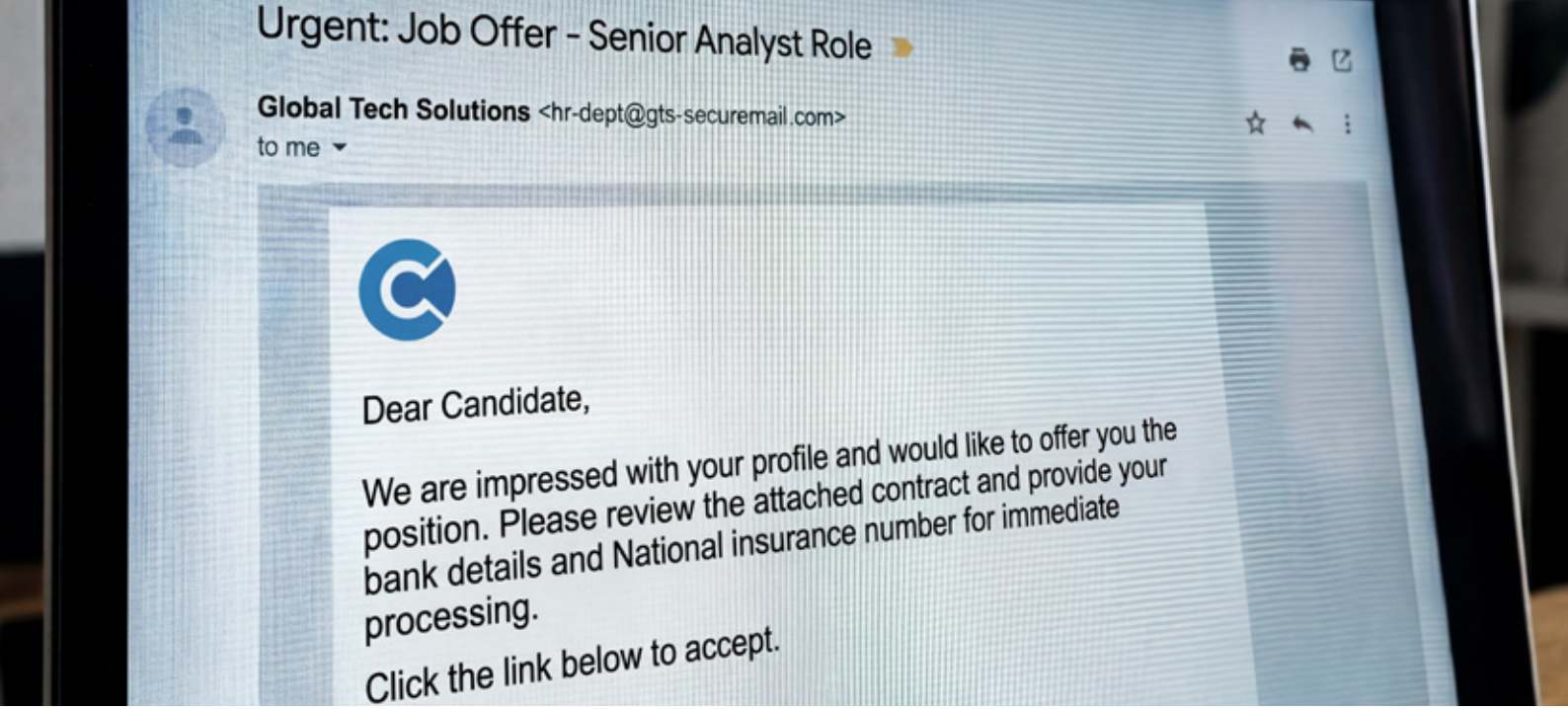
Organised crime groups often need to move money obtained from criminal activities to make it appear as though it's come from a legitimate place. One method they use is recruiting people (knowingly or unknowingly) to help transfer these illegal funds through bank accounts.

Criminals will target individuals; especially students, those looking for quick cash or those looking to work from home, flexibly or part-time. Individuals are told to complete tasks including setting up new bank or crypto accounts, withdrawing cash or transferring money on behalf of others. The individual is ordinarily able to keep a certain percentage of the money transferred as commission.

Criminals target people via social media, messaging apps or even in person. In their fraudulent adverts, they claim there's a legitimate reason for you to transfer money through your account rather than through a company account.

Allowing your accounts to be used in this way is **money laundering** and is illegal. Banks are on the lookout for suspicious transactions. If you move money in this way, your **account can be frozen or closed**, and your name may be blacklisted by banks and credit agencies. This can harm your credit score. You could be investigated by the police and face criminal charges for money laundering which in some cases carry severe penalties including up to **14 years in prison**.





How to protect yourself:

- **Never give anyone the use of your bank account,** bank card or PIN number. Your accounts are for your personal use only.
- **Be sceptical of any job offers or requests that involve receiving or sending money** on someone else's behalf. Legitimate companies do not use personal accounts to do this.
- If someone offers you "easy money" for little work, **check the validity** of it before accepting. Criminals prey on people's hopes for quick, easy cash but this can land you in serious trouble.
- **Research the wider company** and make sure they are genuine.
- If you suspect someone is trying to recruit you to launder money, **disengage and do not participate**. You can **report such approaches** to your bank or to Police Scotland.

If you're in doubt about a job advert, visit www.safer-jobs.com for free advice.

Further Advice

Age Scotland

Age Scotland is the country's largest charity dedicated to helping everyone make the most of later life. They offer companionship, advice and support to older people who need it most. Call **0800 12 44 222** or visit their website at www.agescotland.org.uk

Cifas

UK fraud prevention service Cifas offers Protective Registration to people who have been victims of, or are at risk of, identity theft.

This service flags your personal file so that when Cifas member companies receive an application in your name, they'll conduct extra checks to ensure the application is genuine – www.cifas.org.uk

Citizens Advice Scotland

Citizens Advice provides free, confidential and independent advice to help people overcome their problems. They can help with many issues, from money concerns to problems at work, housing to consumer rights. Call **0800 028 1456** or visit www.citizensadvice.org.uk/scotland/

Companies House

You can obtain details about a company for free online, including:

- Company information, e.g. registered address and date of incorporation
- Current and resigned officers
- Previous company names Insolvency information

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

Cyber Choices

The Cyber Choices network was created to help people make informed choices and to use their cyber skills in a legal way.

The programme is a national initiative co-ordinated by the National Crime Agency and delivered by Cyber Choices teams within Regional Organised Crime Units and Local Police Force Cyber Teams – www.cyberchoices.co.uk

Cyber Helpline

The Cyber Helpline provide free advice and support to individuals in the UK aged 13 or over, and sole traders, on how to recover from cyber security attacks. They provide chatbot and volunteer services as well as a number of guides – https://www.thecyberhelpline.com/

Financial Conduct Authority

The Financial Conduct Authority's aim is to make financial markets work well so that consumers get a fair deal. They regulate the conduct of thousands of companies within the financial sector including some of those related to digital assets.

They also operate an investment and pensions fraud warnings list of companies to avoid and a reporting tool for unauthorised firms.

They can be contacted via their website; www.fca.org.uk or by calling 0800 111 6768. Their Firm Checker tool can be accessed on their website at www.fca.org.uk/consumers/fca-firm-checker

Financial Ombudsman Service

The Financial Ombudsman Service is a free and easy-to-use service that settles complaints between consumers and businesses who provide financial services.

They resolve disputes fairly and impartially including frauds and investments – www.financial-ombudsman.org.uk

Financial Service Compensation Scheme (FSCS)

The FSCS protects the customers of financial services firms which have failed. They provide free compensation claims advice through an online claims service to individuals who are eligible under the FSCS compensation rules – www.fscs.org.uk

Have I been pwned?

"Have I Been Pwned?" is a free website for businesses and individuals to check to see if an email address has been involved in any data breaches. By typing in an email address, you can see if and when it was involved, and where that breach occurred.

This can help people see if their email or password has been made public, and to ensure passwords are changed – www.haveibeenpwned.com

Mail Preference Service

This is a free service enabling UK consumers to stop receiving unsolicited mail by having their home addresses removed from mailing lists.

It is actively supported by Royal Mail, trade associations and the Information Commissioner's Office.

To register for the Mail Preference Service call **020 7291 3310** or visit http://www.mpsonline.org.uk

National Crime Agency (NCA)

The NCA leads the UK law enforcement's fight to cut serious and organised crime. Their website contains information regarding current crime threats and online safety guidance for businesses – www.nationalcrimeagency.gov.uk

National Cyber Security Centre (NCSC)

The NCSC is part of GCHQ and is the UK's lead authority on cyber security. The NCSC's main purpose is to increase cyber security and cyber resilience.

It works with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management.

NCSC also provides incident response to minimise harm to the UK, help with recovery and to learn lessons for the future – www.ncsc.gov.uk/

National Debtline

National Debtline offers free and impartial advice for those struggling with debt. This can be accessed by phone and webchat services between 9am-8pm Monday-Friday and Saturday 9:30am-1pm. They can be contacted on **0808 808 4000** or via webchat on https://www.nationaldebtline.org/ and their website also offers an advice fact sheet.

No More Ransom

The "No More Ransom" website is an initiative by the National High Tech Crime Unit of the Netherlands Police; Europol's European Cybercrime Centre and private cyber security companies. Its goal is helping victims of ransomware retrieve their encrypted data, without having to pay the criminals.

Since it's much easier to avoid the threat than to fight against it once the system is affected, the project also aims to educate users about how ransomware works and what countermeasures can be taken to effectively prevent infection. It can be accessed via www.nomoreransom.org

Online Dating & Discovery Association (ODDA)

The Online Dating & Discovery Association was set up to maintain standards across the online dating industry and reassure users that each member website is working to achieve the highest standards of security for its users.

ODDA members are required to adhere to the membership codes of practice and are committed to providing users with advice, guidance and support in the event of any problems they may encounter when using members websites.

Visit https://theodda.org/

Royal Mail Opt Out Service

Opting out from advertising mail stops all unaddressed items from being delivered by the Royal Mail to your address.

Opting out means no one at the address will receive unaddressed mail items via Royal Mail deliveries. Print a copy of an opt-out form. Complete and sign it, then send it to the address of the form.

The form can be accessed via: https://help.royalmail.com/personal/s/article/How-to-opt-out-of-advertising-mail

Telephone Preference Service (TPS)

TPS is a central opt out register allowing individuals to register their wish not to receive unsolicited sales and marketing telephone calls.

It is a legal requirement that companies do not make such calls to numbers registered on the TPS. To register call **0345 070 0707** or visit http://www.tpsonline.org.uk

Trading Standards Scotland

Trading Standards Scotland are responsible for gathering important intelligence to combat doorstep traders and tackle a number of priorities including eCrimes, internet fraud, and doorstep crime.

To report a matter to your Trading Standards Scotland contact them on **0808 164 6000** or visit www.tsscot.co.uk

UK Finance

UK Finance is the trade association representing the banking and finance industry operating in the UK. It represents more than 250 firms in the UK providing credit, banking, markets and payment related services.

Their website contains a wealth of information on how you can protect yourself and your business from fraud and cybercrime. They can be contacted via www.ukfinance.org.uk

Victim Support Scotland

Victim Support Scotland are an independent charity dedicated to supporting victims of crime in Scotland. They offer free and confidential advice for victims of crime.

You can request support via their online form, their free live chat services or by calling their free helpline **0800 160 1985** www.victimsupport.scot

Contact us – Police Scotland

In an emergency, always dial **999** and to report non-emergency incidents call **101**. Further information about reporting crime can be found on our website - https://www.scotland.police.uk/contact-us/

The scams and frauds pages of the Police Scotland website also provide information to assist in combating fraud and other economic crime – https://scotland.police.uk/advice/scams-and-frauds/

The cybercrime pages of the Police Scotland website also provide information to assist in combating cybercrime – https://scotland.police.uk/advice/cybercrime/

FRAUD

Reporting Fraud

If you think you have uncovered a crime, have been targeted or have become a victim, there are many authorities you can contact for advice or to make a report.

This isn't your fault—criminals are skilled at targeting us.

In the first instance, you should **contact your bank immediately** on a number you know to be correct such as the one listed on your statement, their website or on the back of your debit or credit card.

Report cybercrime and fraud to Police Scotland by dialling **999** in an emergency or **101** in a non-emergency or online at **https://www.scotland.police.uk/contact-us/**

- A crime is in progress or about to be committed
- The suspect is known or can easily be identified in the UK
- The crime involves a vulnerable victim

Every report assists police investigations, provides intelligence, informs national alerts that protect all communities, disrupts criminals and reduces harm.

In the UK you can **forward smishing text messages to OFCOM on 7726** (free of charge) and forward suspicious emails to **report@phishing.gov.uk**

If you have any information on crime and you would prefer not to speak to police, you can call **Crimestoppers anonymously on 0800 555 111** or visit **www.crimestoppers-uk.org**. Crimestoppers are an independent charity.

Don't forget to share your experience with friends and family to make them more aware.

If you are in England or Wales please report to Report Fraud online at **https://www.reportfraud.police.uk/** or by telephone on **0300 123 2040**.

Published with permission of the Metropolitan Police Service. Mayor's Office for Policing and Crime and the Crown, 2026