5TH EDITION

THE LITTLE BOOK OF BIG SCAMS

scamwiseNI
PARTNERSHIP

BIG SCAMS

Gloria Hunniford

I am very pleased to be able to introduce the 5th version of the 'Little Book of Big Scams', hoping to further raise awareness of some of the ever-evolving ways criminals use to scam the public out of hard earned money.

Over recent years, particularly through Rip-Off Britain and other projects, I have come across many experiences of the targeted and sometimes indirect frauds that significantly affect the British consumer and the economy.

As you will read in this excellent booklet, the current types of frauds people are experiencing today can range from the more recognisable face-to-face fraud to those carried out by someone anonymously online. The advances in technology enabling most of us to more easily carry out day to day tasks are frequently exploited by those fraudsters who wish to steal our valuable information or money.

I hope that the information and advice contained in this booklet will empower you to identify potential frauds and prevent the loss of your valuable data to those so intent on stealing it. Also, if you are a victim of fraud this booklet will provide advice on the best course of action to report and remedy the unfortunate situation you may find yourself in. Keep alert!

CONTENTS

PAGE

Chief Superintendent
Simon Walls

We are pleased to bring you 'The Little Book of Big Scams', reproduced by kind permission of The Metropolitan Police Service's Cyber Crime Unit. Since the publication of the last version of the Little Book of Big Scams the pace of scamming has not decreased, nor has the determination of scammers to steal as much money from as many people as possible.

Equally the scammers' sophistication and ability to exploit complex technology has undoubtedly developed. They also continue to groom vulnerable victims through sometimes the threat of arrest or prosecution, sometimes the promise of friendship or more and sometimes the promise of financial reward.

What also remains the same is that scams are not simply an issue for the old or for the vulnerable. There is a scam out there with each of our names on it, as a student looking for a summer job, a shopper looking for a bargain or as a holidaymaker looking for their two weeks in the sun somewhere. Although it is acknowledged and well understood that the impact of a scam for an older and vulnerable victim is likely to be greater and longer term.

While there is much about scams that is a source of frustration and disillusionment, what is truly heartening is the willingness of a wide range of people and bodies to engage with conviction in the scams issues and play their part in protecting our communities from this real risk.

The ScamwiseNI Partnership has led and coordinated this activity in Northern Ireland and put the issue of scams front and centre locally. At last count the Partnership had upwards of thirty members. Members come from the charitable, public, finance, and business sectors and also our churches and youth organisations, among others.

The Partnership exists to make the community scamwise.

I hope you enjoy reading this Little Book of Big Scams. It's an easy and a useful read and will better equip you to spot the scams and the scammers. And never forget, if you can spot a scam you can stop a scam.

SCAMWISENI 4 STEPS AHEAD

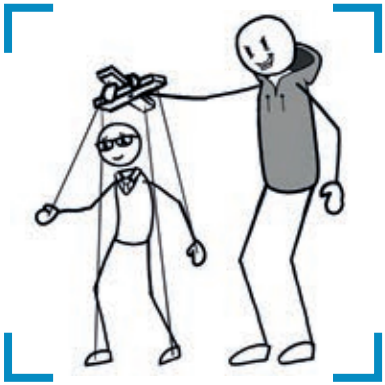
BIG SCAMS

FRAUD ENABLERS

SOCIAL ENGINEERING

All of the frauds described in this book come under Section 2 of the Fraud Act, Fraud by False representation. By this very definition, they involve the criminal scamming the victim by lying, or misrepresenting the situation, and this is commonly referred to as Social Engineering.

Social Engineering is defined as "The clever manipulation of the natural human tendency to trust", and it is this natural inclination that criminals take advantage of. Usually, the criminals' aim is to prey on people's emotions, and get them *feeling* rather than *thinking*. This could either be a sob story, or preying on people's greed. One of the biggest tactics they use is pressure. This could be time related "if you don't do this in 5 minutes, you're going to be in big trouble", or financial "unless you agree to this, you're going to lose thousands". The criminal puts the victim under pressure to decide without allowing them the time to think it through.



How to protect yourself

The best defence against social engineering attacks is knowledge, once you know someone is trying to con you, the con will fail, and reading this booklet should give you that knowledge.

However, even if we're suspicious, we're often bad at saying "no" to people, so if you're uncertain, you can always try these alternatives:

⚠ "I can't make that decision without authorisation. Let me get back to you."

⚠ "I will not make any decisions without speaking to someone first."

However, don't be afraid to simply say "no" to someone. If they're a genuine professional, they won't mind you taking the extra time to verify their identity or offer. If they become pushy or insistent, then odds are fairly high that it's a form of fraud.

ONLINE CRIME

Most people now have access to the internet. We use our home computers, phones and other devices to shop or bank online, contact our friends and relatives, along with numerous other tasks. With all the convenience the internet brings, it is important to be aware of potential online risks.

The vast majority of all frauds now use computers or technology in some way. There are many criminals who take advantage of the anonymity the internet offers to deceive, hack and steal.

There are a number of ways cyber criminals can attack you and your device. They may search the internet to find insecure devices, send an email containing malicious software or even set up fake websites.

How to protect yourself

This doesn't mean we shouldn't use the internet. A few simple security measures can reduce your chances of becoming a victim.

- ⚠ Be wary about the personal information you post online, and ensure you check your privacy settings on social media sites.
- ⚠ Use three random words to make sure your password is strong, e.g. 'FishBoatTulip'.
- ⚠ Storing passwords in your browser is a good tactic.
- ⚠ You can also use a password manager if you want.
- ⚠ Have a strong and separate password for your email account.
- ⚠ If available, set up two-factor authentication on all important accounts.
- ⚠ Use anti-virus software on all devices and update it regularly.
- ⚠ Update your software when new patches are released.
- ⚠ Back up your important data regularly using an external device or cloud storage service.
- ⚠ Secure your tablet or smartphone with a screen lock.

Much more detailed information on cyber crime can be found within our Little Book of Cyber Scams, available free at www.nidirect.gov.uk/publications/little-book-big-scams. Hard copies are also available for free on request.

MONEY MULES (CRIMINAL MONEY LAUNDERING)

Where financial gain comes from crime, criminals use banking systems to move their proceeds i.e. 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 funds or by coercion.

Organised Crime Networks (OCN's) have endeavoured to set up accounts, or gain control of existing accounts for the express purpose of moving the proceeds of crime through a system of accounts for years. This is the Criminal Offence of Money Laundering under the Proceeds of Crime Act 2002. The reason is twofold, to create distance from themselves and the crime they have committed and to make the money appear 'clean' – hence the word laundered – when cashed out.

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.

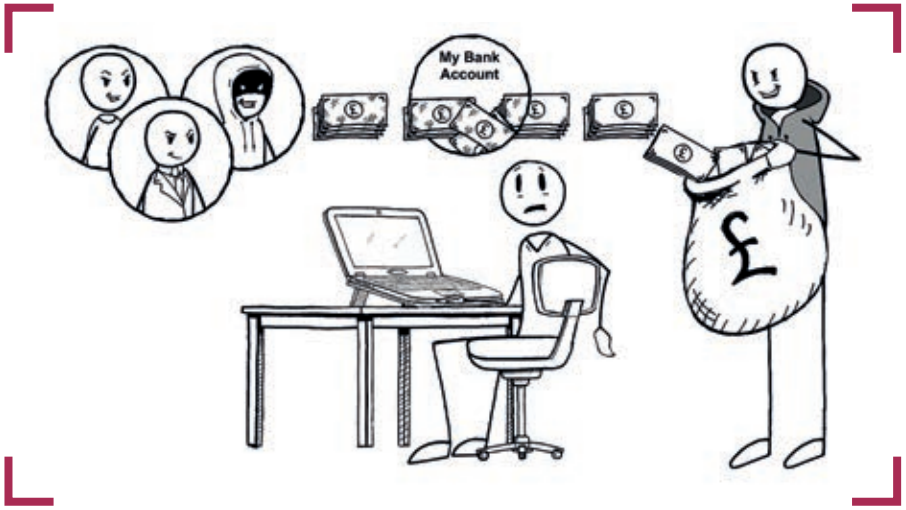
Fraudsters use social media and online forums to take advantage of their fluid acceptance. They post adverts offering the opportunity to make 'easy money' 'free money' or fake jobs using terms like 'Squares' 'AC' 'Flips' 'easy cash schemes', 'no risk money' or 'money transfer jobs'. Criminals rely on the visual representation and enticement of cash, which for a young person can be appealing. 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.

Anyone allowing their bank account to be used by an unauthorised person or have criminal funds go through the account becomes a “Mule”, and breaches the terms and conditions of their Bank account. The bank will close the account and report the account holder to credit agencies. This report effects what, if any credit is awarded and lasts for six years, if there is a guarantor on the account, they may also be affected.

In addition, a Mule could find themselves prosecuted under the Proceeds of Crime Act, and could face up to 14 years in jail.

How to protect yourself

- ⚠ 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 on any advertised jobs.



TYPES OF FRAUD

ADVANCE FEE FRAUD

Advance Fee Fraud is an umbrella term to describe a particular fraud type where the criminal convinces a victim to make upfront payments for goods, services and/or financial gains. But the goods/services don't exist.

Many different types of Advance Fee Fraud utilising various techniques and scams are used by criminals. Some of these (including Romance Fraud and Recruitment Fraud) are covered more in-depth later in this book. However, the numerous different tactics used by criminals means it's worth describing the basic technique behind the fraud; the criminal will offer something to you, but in order to progress, you'll need to pay something up front.

Below is a list of types of Advance Fee Fraud. This list is by no means exhaustive!

⚠ Clairvoyant or Psychic Fraud – The criminal predicts something significant in your future, but they need money to provide a full report.

⚠ Cheque Overpayment Fraud – The criminal overpays for something with an invalid cheque, and asks for change.

⚠ Recovery Fraud – Once you've been a victim of fraud, the criminal contacts you, claiming that they can recover your losses, for a fee.

⚠ Inheritance Fraud – The criminal tells you that you're in line to receive a huge inheritance, but you'll need to pay a fee to release the funds.

⚠ Loan Fraud – The criminal asks you to pay an upfront fee for a loan.

⚠ Lottery Fraud – You're told you've won a prize in a lottery, but you'll need to pay the criminal an admin fee.

⚠ Racing Tip Fraud – The criminal offers racing tips that are "guaranteed" to pay off, for a small fee.

⚠ Rental Fraud – The criminal asks for an upfront fee to rent a property, which may not be theirs, or even may not exist.

⚠ West African Letter Fraud (aka 419 Fraud) – The criminal asks for help moving a large sum of money from one country to another, promising to cut you in, but asks for a payment upfront first.

⚠ Work from home Fraud – The criminal offers you to make easy money working from home, but you need to pay a fee in advance, for business leads, or a website.

⚠ Vehicle Matching Fraud – The criminal contacts you just after you've placed an advert trying to sell something (usually a car). They ask for a "refundable" fee to put you in touch with a non-existent immediate buyer.

How to protect yourself

- ⚠ Be extremely wary about giving money to anyone upfront, especially a stranger, for any reason.
- ⚠ If they claim to be an official, double check their identity, but don't do so using any contact details they give you.
- ⚠ Don't be pressurised into making a decision in that moment. Always take time to think, don't forget to Take 5.

REMEMBER

Criminals will try any lie to get your money.

CAUTION

Don't give money upfront if you have even the slightest suspicion.

THINK

Why should I give this person money? Why have they targeted me?

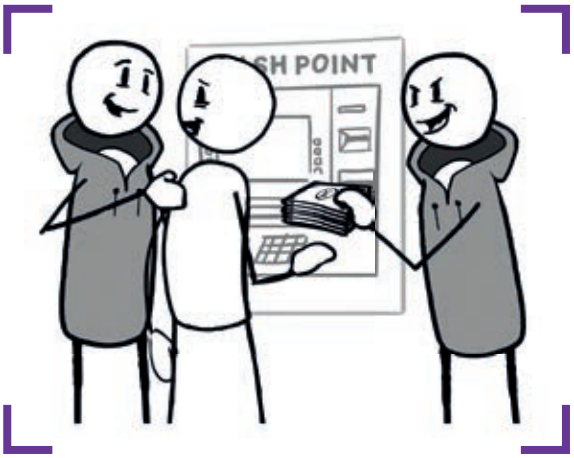
BANKING AND CARD FRAUD – CASH MACHINES

People are targeted at cash machines by criminals who distract users and steal their card or cash. Fraudsters also fit devices to the machines that trap bank cards, copy the card details and record the PIN. You must be vigilant when taking money out of a cash machine and not let anyone distract you.

Criminals may try to see your PIN as you enter it by using a hidden camera or standing nearby. They then attempt to get your card.

They might try and make conversation with you when you are withdrawing money to distract you whilst they or their accomplice takes your card or cash. Criminals have also been known to drop cash on the floor to ask you if it is yours, diverting your attention. They may have fitted a device on the cash machine which either clones your card or retains your card. If your card is trapped in a cash machine by a criminal device, you may leave it unattended to report inside the bank or leave. The criminal will then retrieve the device and your card.

Now the criminal has your card (or a copy) and your PIN.



How to protect yourself

- ⚠ Be wary of anyone approaching you when you are trying to withdraw cash.
- ⚠ Shield your PIN from criminal cameras or prying eyes. Stand close to the cash machine and cover the keypad with your purse, wallet or spare hand.
- ⚠ If there appears to be anything unusual about a cash machine, such as signs of tampering, do not use it and report your concerns.
- ⚠ If your card is retained by a cash machine, report this immediately to your card issuer while still at or near the machine. Store your card issuer's 24-hour contact number in your mobile phone.

BANKING AND CARD FRAUD – CARDS AND CONTACTLESS PAYMENT

Contactless payment is an increasingly popular method of payment, with at least one in three card payments in the UK made using contactless technology. There are many myths that exist relating to the security of this payment system. The information below explains this process, which should ease any concerns you have over this payment method and how it works, whilst giving advice on how to use it safely.

Contactless payment uses a wireless chip containing the user's payment card details which is embedded in a mobile phone or on a bank payment card. This enables users to make payments of up to £30 at stores, cafes and other outlets simply by passing their smartphone or contactless card a few centimetres from a suitable card reader. Some of the security features on this method of payment include the following:

- ⚠ Every contactless card has an in-built security check, which means occasionally you have to enter your PIN number to confirm payment.
- ⚠ Contactless only works when a card or device is within a few centimetres of the reader, making it virtually impossible for details to be intercepted whilst in use.
- ⚠ Whilst a contactless card reader can interrogate a card within 10cm, it will only release the information on the front of the card. For fraud purposes, this is incomplete, and can't even be used to clone the card.

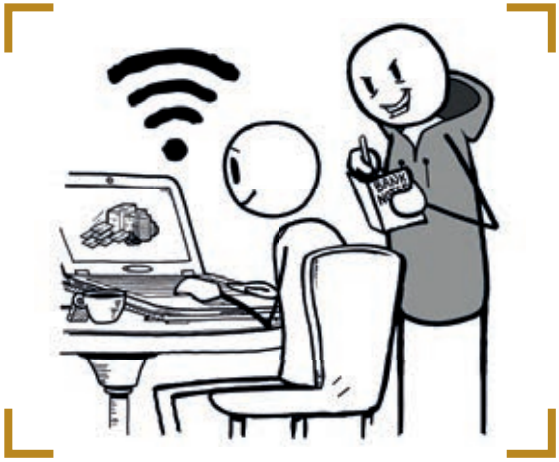
How to protect yourself

- ⚠ Look through all of your bank cards to identify which ones are contactless.
- ⚠ Don't let anyone take your card out of sight while taking a payment – even for just a few seconds. They could be using a skimming device to copy data from your card's magnetic strip, or copying the CCV code on the back.
- ⚠ Monitor your bank statements regularly to ensure that payments have not been taken from your account without your knowledge or permission.
- ⚠ If your contactless payment card or contactless enabled smart phone is lost or stolen, report this to your bank immediately and you should be covered for any subsequent losses.

BANKING AND CARD FRAUD – ONLINE BANKING

The use of online banking or people using banking apps on smartphones and tablets has grown. People use them at home or when they are out and about.

To stay safe while banking online you must protect your password and personal details to stop criminals from accessing your accounts. Many banks provide one-time passcodes sent to your device when setting up new payments. These should never be shared with anyone, even from the bank. If you're speaking to your bank on the phone, and they ask you for it, you are certainly speaking to a criminal, not your bank.



How to protect yourself

- Choose, use and protect passwords and memorable words with great care. Watch the Metropolitan Police's video on passwords at www.met.police.uk/littlemedia for further advice.
- Keep online banking software and banking apps up to date. Always download updates when prompted.
- When logging in whilst in public, take extra care to shield any PIN codes or passwords.
- Always log out of your online banking account or banking app when you have finished using it. Closing the app or web page or turning off your device may not be sufficient.
- Do not use publicly available Wi-Fi networks for banking. It is very difficult to tell if a hotspot is secure.
- Don't share any security codes with anyone.
- If your bank has called you. Take a reference number, and then hang up before recalling on a number you know to be safe after a few minutes to clear the line.

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 even use the name of your broadband provider to sound more legitimate.

The criminals may ask you to complete a number of actions on your computer, and they may even be able to demonstrate an 'error'. 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/years. If you do provide payment details, these may be used to commit further fraud against you.

How to protect yourself

- ⚠ A genuine computer service company will never call you out of the blue regarding issues with your computer. If you receive a call like this hang up straight away.
- ⚠ Never allow anyone to 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.
- ⚠ Most broadband providers offer a free and easy test to measure the speed of your broadband service.
- ⚠ Watch the Metropolitan Police's video on Computer Software Service Fraud at www.met.police.uk/littlemedia.

REMEMBER

Genuine computer service companies don't make these calls.

CAUTION

Don't let anyone remotely access your computer.

THINK

Why are they calling me, there didn't seem to be a problem? How do I know they are genuine?

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 or police. They then ask for your help or say your account is at risk. The ultimate aim of this call is to trick you into parting with your money 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. 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 it is going to be sent off 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 typing in your PIN then handing over your cards to a courier sent to your address (often after you have cut them up as instructed).

- ⚠ 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 of 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.

Criminals have developed their methods further to no longer involve the courier. They may now claim that as a result of the fraud, they are investigating your bank account and therefore ask you to transfer your money into a 'safe account'. They will provide you with the account details and may even say this is set up in your name. This is called Push Payment Fraud (see page 36).

How to protect yourself

- ⚠ Be extremely wary of unsolicited phone calls from your bank or the police, particularly if they are requesting personal information.
- ⚠ End the call, and call back on a different phone line or on a mobile. If this is not possible, wait at least one minute before calling back. Use either the telephone number on your bank card, go to the bank's website or for the police dial '101'.
- ⚠ Speak to friends or family before carrying out any actions. Don't trust claims made by cold callers.
- ⚠ Never hand over your money, bank cards or make purchases following an unexpected call.
- ⚠ Never share your PIN with anyone.
- ⚠ Watch the Metropolitan Police's video on Impersonation Fraud at www.met.police.uk/littlemedia.

REMEMBER

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.

CAUTION

If you receive an unexpected call, hang up and use another phone to call back and confirm identity.

THINK

How do I know they are who they say they are?

DOOR-TO-DOOR FRAUD

Door-to-door scams involve criminals knocking on your door and unexpectedly offering products or services. Fraudsters convince you to pay for goods or work which is often overpriced, of 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 left over 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. Beware of these tactics as these images may not even be your property.
- ⚠ 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. Gas, electricity and water companies may visit to read your meters. Charities may visit to ask for donations and council officials may contact you regarding local issues. Always ask for identification and tell them to wait outside whilst you check this by calling the company or speaking to a relative or friend. If you are calling the company, don't use the phone number on the person's ID card).

How to protect yourself

- ⚠ Always check their identity. If you are not happy about a person's identity, do not let them into your house under any circumstances.
- ⚠ Never leave your front door open/unlocked and unattended, so a second individual can't enter without your knowledge.
- ⚠ Take time to consider your options and research costs from other providers. If in doubt contact your local Trading Standards.
- ⚠ If you feel pressured by any cold caller, have the confidence to be firm and say no.
- ⚠ Legitimate builders do not call door to door.
- ⚠ Call Consumerline following a doorstep caller on 0300 123 6262.

REMEMBER

Take time to consider your options. Don't be pressured into making a quick decision.

CAUTION

Never pay upfront for goods or services you have not received.

THINK

Are they a legitimate company? Why haven't they given you a written quote?

HOLIDAY FRAUD

Millions of people book their holiday online. Whilst you can get some fantastic deals, criminals take advantage of this. They advertise flights, accommodation and other travel services that are not provided or don't exist.

You may only become aware you have been the victim of a scam when you arrive at the airport, or even worse, your destination to find no booking has been made.

The false advertising can be either an entirely fraudulent website or a fraudulent advert posted on a genuine website. Images of the holiday may be used to make the offer seem authentic, however these could have been copied from anywhere on the internet.

Criminals will often ask you to complete the booking away from the site, even offering a further discount for doing so. They may encourage payment by direct bank transfer rather than third party payment services (e.g. Paypal) as this makes it much harder for you to recover your funds.

Fraudsters may even send 'confirmation' emails to convince you the booking has been made.

How to protect yourself

⚠ Where possible, pay for holidays and travel using a credit card. This can provide you with additional financial protection.

⚠ Ensure your booking is covered by a consumer protection scheme such as ABTA (Association of British Travel Agents) and/or ATOL (Air Travel Organiser's Licence). However, their logos can be copied by fraudsters to add credibility to their adverts. Look for the membership number and contact the scheme to confirm if the company you are using is really a member.

⚠ Research any property before you book and look to see if it is advertised elsewhere or has its own website. Be extremely cautious if the prices are significantly different.

⚠ Don't be convinced by photos as they may have been taken from elsewhere on the internet. You can check photos using a reverse image search on the internet through websites like https://www.tineye.com/ or https://reverse.photos/

REMEMBER

If possible, pay by credit card.

CAUTION

Be suspicious of any discount offered for paying by bank transfer, or requests to complete the booking offsite.

THINK

Can I trust the advert? How do I know the booking exists?

IDENTITY FRAUD

Identity fraud involves the misuse of an individual's personal details to commit crime. Your details are valuable to criminals and can be misused by them, or sold on to others. If your data is obtained by criminals it may be used to obtain credit cards or bank accounts in your name, as well as numerous other financial products.

Criminals can also use your stolen information to gain access to the funds in your bank accounts, savings accounts or pension. Your details can be obtained in a number of ways, from letters or bank statements you throw away, to information stolen from your computer or mobile device.

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.

How to protect yourself

- ⚠ Sign up to a reputable credit rating agency. After doing so you will be notified when a credit check is completed using your details. This can identify if someone is using your details without your knowledge.
- ⚠ If you start to receive post from a company or organisation you don't know, find out why it is being sent to you.

- ⚠ Be extremely wary of unsolicited phone calls, emails or text messages claiming to be from your bank or your phone provider. Particularly if they are requesting personal information such as dates of birth or passwords.
- ⚠ Review your bank and credit statements for any suspicious activity.
- ⚠ Have security software installed on your computer and mobile devices to prevent malicious software being downloaded. Make sure the software is kept up to date as prompted.
- ⚠ Do not open attachments or click on links in unexpected emails. This can lead to malicious software being downloaded on to your device or your information being harvested from fraudulent websites you are directed to.
- ⚠ Make sure you dispose of any documents which contain personal information securely (via shredder, or burning etc.)

REMEMBER

Your personal information is valuable and needs protecting.

CAUTION

Be wary of anyone asking you for your private information.

THINK

Why am I being asked to give this information? Is it necessary?

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 do not exist.

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

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

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

It is relatively easy to register a company with Companies House. This does not confirm or endorse that they can provide genuine investments. Indeed, emerging investment markets may be unregulated, making these open to abuse.

Companies may be registered at prestigious addresses, for example Canary Wharf or Mayfair. 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 has to 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 scam. They may be linked to the company who initially defrauded you in the first place and may be targeting you again. This is known as 'Recovery Fraud'.

How to protect yourself

- ⚠ There are no get rich quick schemes. If it sounds too good to be true, it probably is.
- ⚠ Genuine investment companies will not cold call you. Be extremely wary of anyone who does.
- ⚠ Research both what you have been offered, and the investment company. Speak to Trading Standards if you have concerns.
- ⚠ Before investing, check the Financial Conduct Authority register (https://register.fca.org.uk/) to see if the firm or individual you are dealing with is authorised.
- ⚠ Check the FCA Warning List of firms to avoid.

REMEMBER

Don't be pressured into making a quick decision.

CAUTION

Seek independent financial advice before committing to any investment.

THINK

Why would a legitimate investment company call me out of the blue?

ONLINE SHOPPING AND AUCTION SITES

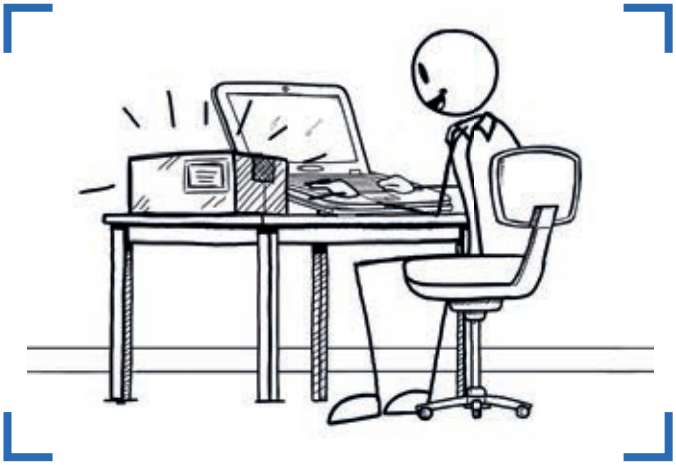
Online shopping can save you time, effort and money. Millions of people use websites such as eBay and AutoTrader to buy new or second hand goods for competitive prices. These sites give you the opportunity to purchase a huge choice of goods from all over the world. However, among the genuine buyers and sellers on these sites, there are criminals who use the anonymity of the internet to offer goods for sale they do not have, or are fake.

In the majority of transactions, the buyer and seller never meet. Which means when making a purchase or sale on a website, you are reliant on the security measures of the site.

Fraudsters will advertise an item for sale, frequently at a bargain price compared to other listings of a similar type. They may have pictures of the item so it appears to be a genuine sale.

A favoured tactic is to encourage buyers to move away from the website to complete the transaction, and the criminal may offer a further discount if you do so. Many websites offer users the opportunity to pay via a recognised, secure third party payment service, such as PayPal, Android Pay or Apple Pay. Read the website's advice and stick to it. Fraudsters might be insistent you pay via bank transfer instead. By communicating and paying away from the website, contrary to their policies, you risk losing any protection you had.

Criminals may also email or contact you if you have 'bid' on an item but not been successful in winning the auction. They will claim that the winning bidder pulled out or didn't have the funds and offer you the chance to buy the item. Once you agree, they will either provide bank details or even insist payment is made via a third party payment service for mutual protection. Once you agree, they 'arrange' this. You then receive a very legitimate looking email which appears to be from the website or a third party payment service directing you how to make the payment. Some are very sophisticated, even having 'Live Chat' functions that you can use to speak to a sales advisor! Unfortunately, you will again be communicating to the fraudster, so beware!



In both these scenarios, once the payment is made, the 'seller' won't send the item. They'll either not reply to you or make excuses as to why they haven't sent the goods.

If they do send the item, they'll send counterfeit goods instead of the genuine items advertised. Again, you may struggle to receive any compensation or resolution to this problem from the legitimate website, as it could be against their policies.

Fraudsters also use e-commerce websites to pose as 'buyers.' If you have an item for sale, they may contact you and arrange to purchase this. It is common for criminals to fake a confirmation that payment has been made. Before posting any item, log in to your account via your normal method (not a link on the email received) and check that you have received the money.

You must also be careful what address you send items to. Fraudsters may ask you to send items to a different address. They may claim they need it sent to their work address or to a friend or family member. 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.

How to protect yourself

⚠ Stay on the website!

⚠ Be wary of offers that look too good to be true.

⚠ Read the consumer advice on any website you are using to make a purchase. Use the recommended payment method, or you may not be refunded for any losses to fraud.

⚠ Research the seller/buyer and any of their bidding history.

⚠ Don't be convinced by pictures, they may have been taken from somewhere else on the internet. You can check photos using a reverse image search on the internet through websites like www.tineye.com or https://reverse.photos/

⚠ Be suspicious of any requests to pay by bank transfer or virtual currency instead of the websites recommended payment methods.

⚠ Never buy a vehicle without seeing it in person. Ask to see the relevant documentation for the vehicle to ensure the seller has ownership.

⚠ If you are selling online, be wary of any emails stating funds have been sent. Always log in to your account via your normal route (not via link in email) to check.

⚠ Watch the Metropolitan Police's video on Online Shopping Fraud at www.met.police.uk/littlemedia.

REMEMBER

Stay on site.

CAUTION

Be wary of paying by bank transfer or virtual currency.

THINK

Why is this item so cheap? Is it a scam?

PAYMENT FRAUD

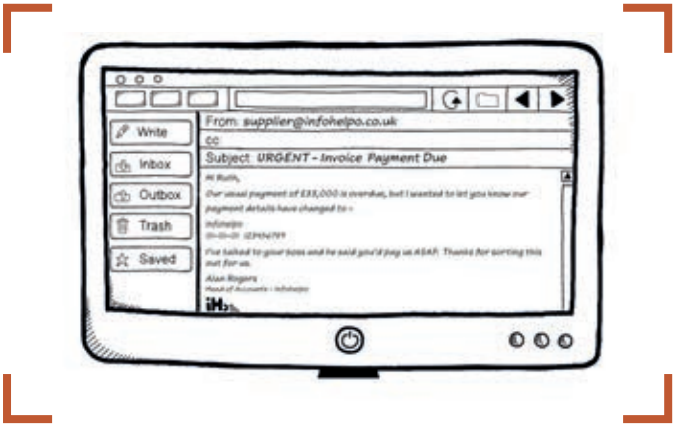
Payment fraud is a specific type of fraud which targets businesses with the intention of getting them to transfer money to a bank account operated by the criminal.

There are two main types of payment fraud, CEO fraud and Mandate Fraud. Both are usually targeted at staff within a company's accounts department and use spoofed sender email addresses (sometimes called Business Email Compromise).

CEO fraud involves an email that claims to be from a senior member of staff within a company such as a CEO (Chief Executive Officer). The email will ask the receiver to make a payment or transfer funds for an ongoing or new business transaction. Often the payment request is marked as urgent and pressure is applied to the receiver to make the payment as soon as possible.

Mandate fraud involves an email which appears to come from a known supplier. The email will request that future payments for products or services are made to a new bank account and give a reason for the account change.

In each instance, the new account will be under the control of the criminal and any funds paid in to it will be lost.



How to protect yourself

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. Ideally, phone them on a number you already have, failing that, double check the email used. Do not use any contact details from the suspicious email. Don't be pressurised by any email, or follow up phone call, as this may be the criminal. Always double check.

However, some criminals are getting wise to this, and so will prep a victim in advance by contacting them a few days or weeks earlier to change any stored phone numbers or emails to their own. So, it's a good idea to double check any contact when change of details occur. Make sure you double check via the original contact details.

Watch the Metropolitan Police's video on Payment Fraud at www.met.police.uk/littlemedia.

REMEMBER

Don't change bank details without double checking.

CAUTION

Sometimes, criminals will call in advance to fraudulently change contact numbers. Check when these change too.

THINK

Why does this payment have to be made?

PUSH PAYMENT FRAUD

Online banking makes managing money easier for the general public, however criminals are taking advantage of this ease of banking and using it to defraud the public.

Criminals can pretend to be from somewhere official, for example, your bank, or the tax office. They contact you via email, phone or social media, and then warn you of fake suspicious or criminal activity on your bank account. They state that they've set up a safe account for you to transfer your funds into. However, this is actually their account.

How to protect yourself

⚠ Be suspicious of a call out of the blue from someone claiming to be from a position of authority.

⚠ Take down the person's details (name, authority, department, branch etc.) and verify using independent source contact details.

⚠ A genuine official from the Police, your bank, HMRC or any other trusted authority will NEVER call you to ask you to verify your personal banking details, PIN or password, or threaten you with arrest.

- ⚠ Never transfer money into another account unless you are 100% certain of the owner of the account.
- ⚠ Your bank will never set up a "safe" account for you.
- ⚠ If you are a victim, contact your bank as soon as possible, as they may be able to help stop the transfer.
- ⚠ Watch the Metropolitan Police's video on Impersonation Fraud at www.met.police.uk/littlemedia.

REMEMBER

Your bank will never set up a 'safe account'.

CAUTION

Unless you definitely know who the account belongs to, it might not be safe.

THINK

Who told me this account was safe? Have I checked their identity?

RECRUITMENT FRAUD

WRITTEN WITH SAFER-JOBS AND THE DISCLOSURE BARRING SERVICE (DBS)

Most people apply for a number of different jobs throughout their working lives. As technology advances, so do the techniques fraudsters use to exploit job seekers during this process.

The majority of these frauds involve the recruiter demanding some kind of payment or fee for Disclosure Barring Service (DBS) checks, training, certification, travel or work permits. The job advert which has attracted applicants is often fake and the recruiter may stop communication once payment is received or ask for more! Information provided to fraudsters by 'applicants' can also be used by criminals to open up bank accounts and loans, known as identity theft.

How to protect yourself

⚠ Applicants should research the company advertising the role to make sure that the job being applied for exists. You should be suspicious if asked to pay for any fees upfront for security checks, visas or training.

⚠ Never phone the company on a premium rate number for an interview, premium rate phone scams are common. You can end up paying a large amount for every minute you are kept on hold. If you are in any doubt visit www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers or research the number online.

- ⚠ Never provide personal details such as your bank account, National Insurance number, date of birth, driving licence or utility bill information during an application process or on your CV.
- ⚠ Do not conduct the whole process online. At some point a job application should lead to a telephone call or face-to-face interview. Be wary of hiring agents who keep solely to email.
- ⚠ Do some research, find out about the company that the job is with. Check landline telephone numbers to confirm the job is real. Use social media and similar sources to dig deeper into the organisation to check their reputation.
- ⚠ If you're in doubt about a job advert, visit www.safer-jobs.com for free advice.

REMEMBER

Your personal information is valuable, protect it.

CAUTION

Do some research to check if the company exists and if they are really advertising the role.

THINK

Why am I being asked to make upfront payments?

ROMANCE AND DATING 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 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 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.

How to protect yourself

- ⚠ 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. You can check photos using a reverse image search on the internet through websites like https://www.tineye.com or https://reverse.photos.
- ⚠ 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 using you to launder money.
- ⚠ Talk to family and friends for advice, even if the other party is asking you to keep the relationship secret.
- ⚠ Watch the Metropolitan Police's video on Romance Fraud at www.met.police.uk/littlemedia.

REMEMBER

Stay on site! Never send money to someone you have not met in person, or receive/ transfer money on their behalf.

CAUTION

Be wary of continuing the relationship away from the dating website you initially made contact on.

THINK

Why are they so quick to declare their love for me? How do I know they are telling me the truth?

SCAM MAIL

Many victims of scam mail, also known as mass market fraud, are drawn in by the thrill of a guaranteed win. You will part with money in order to claim a prize that does not exist. Often, victims of this type of crime are elderly or vulnerable. They are targeted because they may live alone or have access to significant savings or pension funds.

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

The letters may claim you have won a prize draw; competition or lottery you have not even entered. The letters will be personally addressed to you, giving the illusion that 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 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 scam mail, to be inundated with more. After this response your details will be added to a 'victims list' that other fraudsters have access to.

How to protect yourself

⚠ You cannot win a competition or lottery you have not entered! If you are asked to pay an upfront fee for such a 'win' do not pay!

⚠ If you purchase goods in response to a mail offer, make sure you review your bank or credit card statements.

⚠ Any doubts, speak to a friend or relative.

REMEMBER

You cannot win a prize if you haven't entered.

CAUTION

Be wary of anyone asking you for your private information.

THINK

Why am I being asked to make upfront payments?

TICKETING FRAUD

Getting tickets to see your favourite band, football team or theatre production can be extremely difficult as tickets sell out quickly. Criminals take advantage of this by offering tickets for sale that do not exist or are fake.

Most event tickets are sold via reputable websites operated by promoters, the event venue or other official agents. Many tickets are also offered for sale on secondary resale sites. Fraudsters set up fake ticket sales websites, place adverts on secondary resale sites or use social media to sell tickets they do not have.

Once a payment is made, you will either not receive the tickets, or the tickets you receive will be fake or non-transferrable. When you arrive at the venue you will not get in.

Some tickets are non-transferable and can only be used by the person who initially purchased them. In many cases, unauthorised resale of these tickets is illegal.

How to protect yourself

- ⚠ Buy tickets from the event promoter, venue box office, official agent or a reputable ticket exchange site or app.
- ⚠ Where possible, pay for tickets using a credit card as this offers additional financial protection.
- ⚠ Be suspicious of requests to pay by bank transfer.
- ⚠ Be wary of paying for tickets where you are told someone will meet you at the event with your tickets as they may not arrive.
- ⚠ 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.
- ⚠ For further information on buying tickets safely visit the STAR website.

REMEMBER

The site you are using could be fake.

CAUTION

Use your credit card to pay, this could offer you additional protection.

THINK

How can I check the tickets are real?

BIG SCAMS

WHAT TO DO IF YOU GET SCAMMED

GET HELP AND REPORT A SCAM

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

Reporting crime, including fraud, is important. If you don't tell the authorities, how do they know it has happened and how can they do anything about it? Remember that if you are a victim of a scam or an attempted scam, however minor, there may be hundreds or thousands of others in a similar position. Your information may form part of one big jigsaw and may be vital to completing the picture.

Reporting fraud

Fraud can be reported directly to the Police Service of Northern Ireland by calling 101 (999 in an emergency) and by visiting your local police station.

Action Fraud

Reporting online: www.actionfraud.police.uk
Telephone reporting: 0300 123 2040

Unless

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

If this is the case you should contact police directly either by dialling 999 in an emergency, dialling 101 in a non-emergency or visiting your local police station.

If you have any information on any 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 is an independent charity.

OTHER CONTACTS

There are many other organisations out there dedicated to fighting fraud and cyber crime, or providing help and advice to individuals and businesses.

Action Fraud

Action Fraud is the UK's national reporting centre for fraud and cyber crime. If you have been scammed, defrauded or experienced cyber crime, you should report this directly to Action Fraud by telephone or via their website for full reporting information. The Action Fraud website also provides fraud and cyber crime prevention advice and details of the latest scams.

Call 0300 123 2040 or visit www.actionfraud.police.uk

Age UK

Age UK 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 169 8787 or visit their website at www.ageuk.org.uk

Alzheimer's Society

A national charity providing advice and support for people affected by dementia.

Call 0300 222 1122 or visit www.alzheimers.org.uk

The Association of British Travel Agents (ABTA)

ABTA is the largest travel trade association in the UK with over 1200 members. All ABTA members must follow ABTA's strict code of conduct and if they breach the code they can be fined or have their membership withdrawn. Consumers who book holidays through ABTA members are financially protected in the event of a company failure.

Visit www.abta.com

Cifas

UK fraud prevention service CIFAS offers Protective Registration to people who have fallen victim to, 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 that the application is genuine.

Visit www.cifas.org.uk

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
- Document images
- Mortgage charge data
- Previous company names Insolvency information

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

Consumer Council

The Consumer Council provide free, independent support and advice for all consumers and businesses in Northern Ireland. We also have powers to investigate complaints about energy, water, transport and postal services and undertake research to understand local consumer issues.

Visit www.consumercouncil.org.uk

Crimestoppers

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

Cyber Aware

Cyber Aware provides cyber security advice for small businesses and individuals, such as using strong passwords made up of 'three random words' and always downloading the latest software and app updates, that can help you protect your devices from cyber criminals.

Visit www.cyberaware.gov.uk

Disclosure and Barring Service (DBS)

The Disclosure and Barring Service (DBS) provides different types of checks. Some jobs require standard or enhanced checks, essentially a criminal record check, and it is up to an employer to assess whether a role is suitable for this type of check. But you can check whether the job you are applying for requires this type of check by using the DBS eligibility tool.

Visit www.gov.uk/find-out-dbs-check

Financial Conduct Authority (FCA)

The FCA's aim is to make financial markets work well so that consumers get a fair deal. To do this they regulate the conduct of more than 56,000 businesses who operate within the financial sector. Their work to protect consumers covers a wide range of activities including ensuring that a firm has its customers at the heart of how it does business, giving them appropriate products and services, and putting the customer's financial protection above the company's profits or remuneration.

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

Friends Against Scams

Friends Against Scams is a National Trading Standards Scams Team initiative, which aims to protect and prevent people from becoming victims of scams by empowering people to take a stand against scams. Anybody can join Friends Against Scams and make a difference in their own way.

Visit www.friendsagainstscams.org.uk to find out more.

Get Safe Online

Get Safe Online is a good source of online safety advice for the general public and small businesses. The advice it provides can help safeguard against fraud and online threats helping to provide a positive experience of the internet. Get Safe Online works closely with the Metropolitan Police, other UK Police forces and law enforcement agencies and industry regulators to provide up to date crime prevention advice and alerts.

Visit www.getsafeonline.org

Hourglass NI

A specialist charity working exclusively to protect and prevent the abuse of older people, with dedicated staff in each of the four UK nations.

Tel: 0749 666 3816
Helpline: 080 8808 8141
Web: www.wearehourglass.org.uk
Email: enquiries@wearehourglass.org

Insolvency Service

The Insolvency Service is an executive agency of the Department of Business Innovation and Skills (BIS). They have the power to investigate Limited companies where they have received information that suggests serious corporate abuse. This may include allegations of serious misconduct, fraud, scams or sharp practice.

To complain about a limited company that is still trading call 0300 678 0015 or visit www.gov.uk/government/organisations/insolvency-service

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 www.mpsonline.org.uk

National Cyber Security Centre (NCSC)

The National Cyber Security Centre is part of GCHQ, it provides advice and intends to make the UK the safest place to live and do business online.

Visit www.ncsc.gov.uk

NI Cyber Security Centre

The NI Cyber Security Centre is setup to develop a cyber safe, secure and resilient Northern Ireland. Through engaging with people and organisations informing them of the majority of cyber threats and in encouraging the adoption of good cyber practices to help them be safe and secure online and be better prepared to recover from cyber incidents and continually improving the resistance and resilience of Northern Ireland to cyber threats.

Visit www.nicybersecuritycentre.gov.uk

The Office of Care and Protection (OCP)

The Office of Care and Protection (OCP) is responsible for the management of the financial affairs of people in Northern Ireland who, through mental disability, are incapable of managing their own finances.

It does this through:

- The supervision of Controllers appointed by the Office of Care and Protection (OCP)
- The registration of Enduring Powers of Attorney (EPAs)
- Enquiries into allegations of financial abuse reported to the Office of Care and Protection (OCP)

For more information contact:

The Office of Care and Protection
1st Floor Royal Courts of Justice
Chichester Street PO Box 410
Belfast BT1 3JF

Tel: (028) 90724733/90724730
Email: ocp@courtsni.gov.uk
Web: www.courtsni.gov.uk

Online Dating Association (ODA)

The Online Dating Association was set up to maintain standards across the industry and reassure users that each member website was working to achieve the highest standards of security for its users. ODA 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 www.datingagencyassociation.org.uk

Royal Mail Opt Out Service

Opting out from Royal Mail Door to Door 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. If you wish to opt out of receiving Door to Door mail items send your name and address details to Freepost ROYAL MAIL CUSTOMER SERVICES or email your name and address to: optout@royalmail.com. You will then be sent an opt-out form to your address, which you must sign and return.

Visit https://personal.help.royalmail.com/app/answers/detail/a_id/293

Royal Mail Scam Mail

If you think you or a family member is receiving scam mail you can report it to the Royal Mail. Write to Royal Mail at Freepost Scam Mail or call on 03456 113 413 or email at scam.mail@royalmail.com

SAFERjobs

SAFERjobs is a charity originally set up by the Metropolitan Police in 2008 with the objective to protect job seekers. It offers free advice to jobseekers and agency workers to ensure people do not fall foul of fraud or illegal practice. Jobseekers are advised to look for recruiters who partner with SAFERjobs for a safer job search.

Visit www.safer-jobs.com

Secure Tickets from Authorised Retailers (STAR)

STAR is the leading self-regulatory body for the entertainment ticketing industry across the United Kingdom. STAR members include major UK ticket agencies as well as numerous venues and box offices in London and across the country. STAR offers general advice and information on ticket buying and provides a dispute resolution service for customers who have an unresolved problem with their purchase from a STAR member.

Visit www.star.org.uk

Stay Safe Online

Powered by the National Cyber Security Alliance, Stay Safe Online builds strong public/private partnerships to create and implement broad-reaching education and awareness efforts. It empowers users at home, work and school with the information they need to keep themselves, their organisations, their systems and their sensitive information safe and secure online and encourage a culture of cybersecurity.

Visit www.staysafeonline.org

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 www.tpsonline.org.uk

The Silver Line

The Silver Line operates the only confidential, free helpline for older people across the UK that's open 24 hours a day, seven days a week. They also offer telephone and letter friendship schemes where volunteers are matched with older people based on their interests; facilitated group calls; and help to connect people with local services in their area.

To contact the Silver Line call 0800 4 70 80 90 or visit www.thesilverline.org.uk

Think Jessica

Think Jessica is a charity set up to protect elderly & vulnerable people from scams which come through the postal system and criminals who contact them by telephone. They offer advice and support to victims of mass marketing fraud as well as assistance to friends and relatives of those that have been scammed.

Visit www.thinkjessica.com

Trading Standards

National Trading Standards is responsible for gathering important intelligence from around the country to combat rogue traders and tackle a number of priorities. These priorities currently include mass marketing and internet scams to other enforcement issues that go beyond local authority boundaries.

To report a matter to your local Trading Standards service contact 0300 123 62 62 or visit https://www.economy-ni.gov.uk/topics/consumer-affairs

UK Finance

UK Finance is responsible for leading the collective fight against financial fraud on behalf of the UK payments industry. Their membership includes banks, credit, debit and charge card issuers, and card payment acquirers in the UK. Their website offers information about the various types of payment fraud, as well as helpful tips and advice on how to minimise your chances of becoming a victim, and what to do if you become a victim.

Visit www.ukfinance.org.uk

REDUCING THE DAMAGE

Although it may be hard to recover any money that you have lost to a scam, there are steps you can take to reduce the damage and avoid becoming a target again.

The quicker you act, the more chance you have of reducing your losses.

Report a scam

By reporting the scam (see page 46), we will be able to warn other people about the scam and minimise the chances of the scam spreading further. You should also warn your friends and family of any scams that you come across.

Scammers are quick to identify new ways of conning people out of their money. Be aware that any new scheme or initiative will quickly be targeted.

Finally, remember that this booklet does not contain all the answers. To avoid being a victim you need to be aware that someone who is not suspicious and has a trusting nature is a prime target for a criminal.

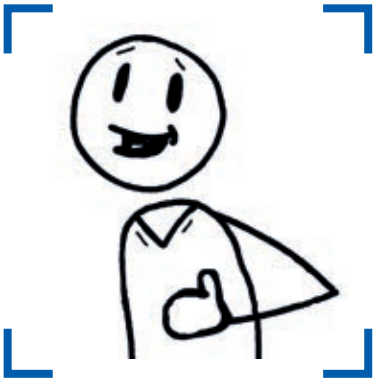
Don't be afraid, but be aware. Don't be scared, be sceptical. And above all, remember if it sounds too good to be true it probably is!

For more information

An audio, 'easy read' and E-version of the original booklet is available on our website www.psni.police.uk/crime/fraud

If you are a member of the public or organisation and reside in Northern Ireland you can find an online copy of this book on our website www.psni.police.uk/crime/fraud If you would like more hard copies of the book, contact your local PSNI Crime Prevention Officer.

The Metropolitan Police Service Cyber Prevention Team have provided many other police forces with the necessary details to print further copies of their own. If you reside outside of the Northern Ireland area then contact your local police force who may be printing their own version.



REMEMBER: financial institutions, utility companies, law enforcement, HMRC, internet & telecoms providers or other public bodies:

- Will **NEVER** ask for payment in vouchers.
- Will **NEVER** ask you to transfer money because your account is compromised.
- Will **NEVER** threaten you over the phone, by letter or email for not paying a fee.
- Will **NEVER** threaten arrest if payment isn't made immediately.
- Will **NEVER** ask for money for a 'free gift', 'admin fee' or as part of a promotion.
- Will **NEVER** ask to reveal your account security codes or online passwords in full.
- Will **NEVER** call out of the blue and ask for remote access to your computer or devices or to download software.
- Will **NEVER** inform you about tax returns by email, text or voicemail.

If you think you have been the victim of a scam

helpful contacts

Department for the Economy
www.economy-ni.gov.uk

Trading Standards
Consumerline: 0300 123 6262
www.nidirect.gov.uk/consumerline
consumerline@economy-ni.gov.uk

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Action Fraud
Tel: 0300 123 2040
actionfraud.police.uk

CALL THE POLICE 101
IN AN EMERGENCY ALWAYS CALL 999

Police Service of Northern Ireland
Non-emergency 101
Emergency 999

We would like to thank the Metropolitan Police Service Cyber Crime Unit and their partners for their time and effort in producing this booklet.

scamwiseNI
PARTNERSHIP

Published by the Metropolitan Police Service