

THE LITTLE BOOK OF

**BIG**

**SCAMS**



**JUST REMEMBER:  
IF IT SOUNDS TOO  
GOOD TO BE TRUE,  
IT PROBABLY IS.**

The Metropolitan Police Service's  
Operation Sterling Team would like to  
thank the following for their time and  
effort in assisting us with this booklet:

Australian Competition and  
Consumer Commission  
The National Fraud Authority  
UK Payments  
The Insolvency Service  
Marilyn Baldwin from the  
Think Jessica Charity  
Brenda Parkes



One of the mysteries of the con-man is why he bothers (I say he, but of course there are plenty of con-women who are just as unscrupulous). He is often energetic, imaginative and ambitious, so why doesn't he build up a decent, respectable business instead of robbing hard-working people? I suppose it's because con-men (and I've met many over my years in consumer protection) all regard the people they deceive simply as walking wallets, to be ruthlessly squeezed, emptied, and then thrown away.

So the con-men will shamelessly lie to us, try to tempt us with "something for nothing", "too good to be true" offers – like the "show house" discount for double glazing or central heating, or the "million pound lottery" he pretends you have won and so on. And he gambles on the fact that when we discover that we've fallen for his blatant swindle, we will be too ashamed to report him to the police or the Trading Standards officers.

I bring you good news. In this excellent booklet, the police are arming us with the best of all weapons to defend ourselves, that is, good information and a timely warning. I urge you to read this booklet, even if you think you could never fall for the con-men's tricks. Bright people, honest people, find it difficult to believe that swindles can arrive through your letterbox, in your inbox, on your doorstep. But they can, alas, and they do, and scams like the ones described in this booklet deceive good people into losing millions of pounds every year.

So congratulations to the dedicated police team who have created this booklet because they are determined to protect us, and prevent the con-men succeeding. And enjoy this booklet, it's an excellent read and it could save you a great deal of money you can't afford to lose.

*Esther Rantzen*

## CONTENTS

- 1** Introduction
- 3** Myth Busters
- 4** 10 Golden Rules
- 5** Identity Fraud
- 8** Mass Market Fraud – Scam Mail
- 10** Investment Scams
- 12** Door-to-Door Scams
- 14** Dating and Romance Scams
- 16** Banking and Payment Card Scams
- 18** Mobile Phone Scams
- 20** Health and Medical Scams
- 22** Internet Scams
- 24** Psychic and Clairvoyant Scams
- 26** Frequent Scamming Tools
- 29** Fraud is Not a Victimless Crime
- 32** Handy Hints to Protect Yourself
- 36** What to do if You Get Scammed  
Contacts and Reporting Advice



**Every year, the British public loses billions of pounds to scammers who bombard us with online, mail, door-to-door and telephone scams.**

Scams (or frauds) are often difficult to investigate; they can be complicated and often involve many people (both victims and suspects). They can take a lot of resources to investigate and courts can find it difficult to convict suspects because of the grey area that exists between dishonesty and sharp practice.

Prevention through awareness is therefore a vital strand in combating scammers.

The Metropolitan Police Service's Operation Sterling Team is pleased to bring you the **Little Book of BIG Scams**. We were inspired by *The Little Black Book of Scams*, originally created by the Australian Competition and Consumer Commission as inspiration. We hope this booklet will increase your awareness of the vast array of scams that are being used and teach you some easy steps you can take to protect yourself. It should be seen as a general guide to many of the scams currently operating in the UK.

## **Scams do not discriminate**

Scams target people of all backgrounds, ages and income levels. Fake lotteries, investment frauds and romance scams are some of the favoured means of separating the unwary from their money. New varieties of these scams appear all the time.

Operation Sterling has seen the devastating effects scams can have on people and their families. One of the best ways to fight scammers is to help you take steps to prevent yourself from being caught out in the first place.

Some adults may be especially vulnerable to financial abuse. Consider liaising with your local Social Services safeguarding adults department if you are concerned about someone you know who may be vulnerable (when contacting your local Social Services, ask for adult social care). Partner agencies can work together to keep an adult at risk safe.

### Protect Yourself

If you want to stay on top of scams, visit our Fraud Alert website <http://www.derbyshire.police.uk/scams> which contains current information on different scams targeting consumers. It also provides you with tips on guarding yourself against scams, new scam stories, scam alerts and advice on reporting scams.

**JUST REMEMBER:  
IF IT SOUNDS TOO  
GOOD TO BE TRUE,  
IT PROBABLY IS.**



**Being aware of these common myths will minimise your chances of being scammed.**

**All companies, businesses and organisations are legitimate because they are approved and monitored by the government.**

**THIS IS NOT ALWAYS TRUE**

Whilst there are rules about setting up and running a business or a company in the UK, scammers can easily pretend to have approval when they don't. Businesses that do have approval to operate could still try and scam you by acting dishonestly. Just because a business looks legitimate does not mean that it is.

**All internet websites are legitimate.**

**THIS IS NOT ALWAYS TRUE**

Websites are easy and cheap to set up and there are very few checks in place to ensure a website is legitimate. Many are not.

**There are short cuts to wealth that only a few people know.**

**THIS IS NOT ALWAYS TRUE**

Ask yourself the question: if someone knew a secret to instant wealth, why would they be telling their secret to others?

**Scams involve large amounts of money.**

**THIS IS NOT ALWAYS TRUE**

Sometimes scammers target a large number of people and try to obtain a small amount of money from each person.

**Scams are always about money.**

**THIS IS NOT ALWAYS TRUE**

Some scams are aimed at stealing your personal information which can then be used fraudulently.

# 10 GOLDEN RULES

**Remember these 10 golden rules to help you beat the scammers.**

- 1 There are no guaranteed get-rich-quick schemes.**
- 2 Do not agree to offers or deals straight away. If you think you have spotted a great opportunity, insist on time to obtain independent/legal advice before making a decision.**
- 3 Do not hand over money or sign anything until you have checked the credentials of the company that you are dealing with.**
- 4 Never send money or give bank or personal details to anyone you do not know or trust. This includes sending money abroad and using methods of payment that you are not comfortable with.**
- 5 Log directly on to a website that you are interested in rather than clicking on links provided in an email.**
- 6 Do not rely on glowing testimonials: find solid independent evidence of a company's success.**
- 7 Always get independent/legal advice if an offer involves money, time or commitment.**
- 8 If you spot a scam or have been scammed, report it and get help. Contact ActionFraud on 0300 123 2040 or online at [actionfraud.police.uk](http://actionfraud.police.uk) or the Police in your area.**
- 9 Always remember: scammers are cunning and clever. They know how to manipulate you to produce the response they want.**
- 10 Be suspicious. If you are unsure about anything, seek independent/legal advice.**

**Identity Fraud is often quoted as ‘Britain’s fastest growing crime.’ It involves the misuse of identity information in order to commit crime. Your personal information is very valuable. Stolen details can be misused and/or sold on to others.**

Victims of identity fraud often report a great deal of stress and cost in trying to clear matters up and may never establish how their details have been obtained.

For more information on the above visit [www.identitytheft.org.uk](http://www.identitytheft.org.uk)



## Protecting your Address:

- ⚠️ If you start to receive post for someone you don't know find out why.
- ⚠️ Register to vote at your current address. Lenders use the electoral roll to check who is registered as living at a particular address.
- ⚠️ When registering to vote, tick the box to opt out of the 'Edited' register to prevent unsolicited marketing mail. (This does not affect credit checks).
- ⚠️ Sign up with the Mail Preference Service to prevent marketing letters. (Details on how to do this are at the back of the booklet).
- ⚠️ Protect mail left in communal areas of residential properties.
- ⚠️ Re-direct your mail when moving home.

### Protecting your Bank Accounts:

- ⚠ Regularly check statements and chase up any statements that are not delivered when expected.
- ⚠ Shred, using a cross cut (confetti) shredder or tear up into small pieces anything containing personal information.
- ⚠ Sign up with a credit reference agency for alerts.
- ⚠ Regularly check your credit reports from a credit reference agency.
- ⚠ Consider signing up to American Express SafeKey, MasterCard SecureCode or Verified by Visa when you receive your cards, even if you do not intend to use your cards on line - this protects you if your card or details are lost or stolen.
- ⚠ Beware of unsolicited phone calls, letters and emails pretending to be your bank, or other financial institution and asking you to confirm your personal details, passwords and security numbers.
- ⚠ If you think someone is misusing your bank account details then report it to your bank.

### Protecting your Phones:

- ⚠ Sign up with the Telephone Preference Service to prevent marketing phone calls (Details on how to do this are at the back of the booklet).
- ⚠ If using a 'smart' phone install anti-virus software on it.
- ⚠ Never reply to unsolicited texts, e.g. texts referring to accident claims even to get them stopped. Simply delete them.

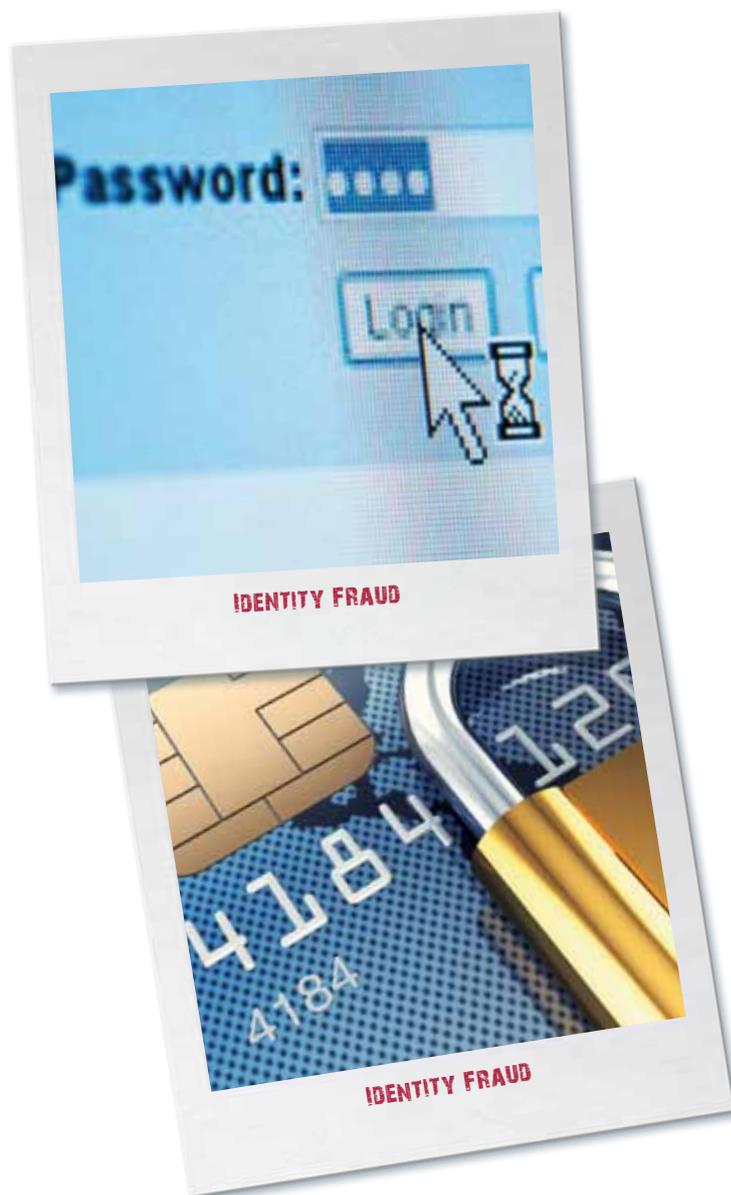
### Protecting your Computer:

- ⚠ Keep your computer security programs (antivirus, anti-spam) up to date.
- ⚠ Restrict the amount of personal information that you disclose when online.
- ⚠ Don't fall for online scams, scam letters via email, advance fee or other internet-related frauds.
- ⚠ Know how to verify secure web sites if making financial transactions. You can do this by looking at the address line. Normally it will start with http but when you log into a secure site

this will change to https for example; <http://www.mybank.com> is the address of mybank, but if you want to go to the transactions page you log in and the address bar will change to something like <https://mybank/login.com>. The address bar may also change colour. A padlock will also appear in either the bottom left or bottom right corner of the browser, not in the website. If you have received an email claiming to be your bank, requesting that you contact them, consider the legitimacy of such an email. If you are unsure, do not use the link in the email you have received. Open another window in your browser and visit your bank's website using your normal method.

**For reporting advice  
please see pages 36 and 37.**

**YOUR PERSONAL  
INFORMATION IS  
VALUABLE:  
BE VIGILANT IN  
PROTECTING IT.**



# MASS MARKET FRAUD – SCAM MAIL

**Many people in the UK and overseas are drawn by the thrill of a surprise win and find themselves parting with large amounts of money in order to claim fake prizes. Large numbers of victims, often the elderly and vulnerable, fall for Mass Market scam mail.**

## What you should know

- ⚠️ You cannot win money or a prize in a lottery if you have not entered it. You cannot be chosen at random if you do not have an entry.
- ⚠️ Many Mass Market scams will trick you into parting with money or providing your banking or personal details in the belief that you will win a cash prize. You do not have to pay a fee to claim a legitimate prize.
- ⚠️ It only takes one time to respond and you will be inundated with scam mail. Your name and address will be included on what's known as a 'Sucker's List' and you will receive large amounts of mail on a daily basis.
- ⚠️ A fake prize scam will tell you that you have won a prize or competition. You may receive 'confirmation' of this by post, email or text message. There will often be costs involved in claiming the prize and even if you receive a prize it may not be what was promised to you.
- ⚠️ You may be offered a dream job but prior to starting you may be asked to pay for taxes, visas, 'anti-terrorism certificates' or any other advanced fee.
- ⚠️ Be aware that items advertised in the post you receive may be marketed as 'High Quality Exclusive Goods' but in reality can be extremely poor value for money.

**For reporting advice  
please see pages 36 and 37.**



**MASS MARKET FRAUD - SCAM MAIL**



**MASS MARKET FRAUD - SCAM MAIL**

**BIG SCAMS**

**REMEMBER**

Genuine lotteries will not ask you to pay a fee to collect your winnings.

**CAUTION**

Never send money abroad or to someone you don't know and trust.

**THINK**

Don't provide banking or personal details to someone you don't know and trust.

**INVESTIGATE**

Examine all of the terms and conditions of any offer very carefully.

**The average victim of an investment scam loses £20,000. Also known as boiler room frauds – the ‘boiler room’ refers to a rented space from which salespeople call hundreds of potential victims each day, using high pressure sales techniques.**

Investments where fraud is commonplace are land, wine, carbon credits, gold and jewels as well as stocks and shares.

## What you should know

- ⚠ Scammers will cold-call you normally by telephone and try to sell you investments that will supposedly lead to huge financial gains. In reality they either do not exist or are worthless.
- ⚠ Often the scammers will give you details that you might think only a genuine investment company will have. They may have details of previous investments you have made, shares you hold and know your personal circumstances. Be aware the scammers will do their homework and make it their business to know as much about you as possible.
- ⚠ The scammers will often call you a number of times slowly developing a friendly relationship. If you respond in anyway they will persist, build trust and eventually persuade you to part with your money. Having obtained some money from you, they will probably call again and try to persuade you to ‘invest’ further money, perhaps in a different commodity.
- ⚠ Scammers may say they are from a well-known and reputable investment company, some will say they are stockbrokers and some pretend to be investors. Always seek independent/legal advice before you commit to any investment.

**For reporting advice  
please see pages 36 and 37.**

# BIG SCAMS

<b>REMEMBER</b>	Do not respond to callers trying to sell you investments. Simply hang up the telephone.
<b>CAUTION</b>	Don't let the company pressure you into buying because they say the offer won't be there tomorrow. Hang up and take a day or two to consider your options.
<b>THINK</b>	Exercise considerable caution when investing your money especially in land, carbon credits, wine, jewels etc.
<b>INVESTIGATE</b>	Always seek independent/legal advice before committing to any investment.



Many legitimate businesses sell products door-to-door (windows, solar panels, cleaning products, home maintenance etc.). Gas, electricity and water companies will also visit to read meters. In addition, charities will visit to ask for donations or post collection bags for you to fill and leave out for collection.

However, scammers also do the above to part you from your money, gain entry to your home to steal or profit by posing as charities in order to collect donations.

## What you should know

- ⚠ Door-to-door scams involve selling goods or services that are not delivered or are very poor quality. You won't get value for money and you may get billed for work you didn't want or didn't agree to.
- ⚠ Some scammers conduct surveys so they can obtain your personal details or disguise their real intent to sell you goods or services you don't want or need (e.g. unnecessary roofing work or patio replacement).
- ⚠ Door-to-door sales are normally uninvited. BUT, they MUST leave if you ask them to.
- ⚠ Even when a genuine business and product is being sold, unscrupulous employees can sometimes still act illegally.

**BE SUSPICIOUS**

**For reporting advice  
please see pages 36 and 37.**



**DOOR-TO-DOOR SCAMS**



**DOOR-TO-DOOR SCAMS**

**BIG  
SCAMS**

<b>REMEMBER</b>	If someone knocks at your door, always examine and check their identification.
<b>CAUTION</b>	Never let anyone in your house unless they are someone you know and trust.
<b>THINK</b>	Don't immediately agree to any offer involving a significant amount of money, time or commitment. Seek independent/legal advice first.
<b>INVESTIGATE</b>	If you are interested in what a door-to-door salesperson has to offer, take time to find out about their business and their offer. Shop around to make sure you are getting a good deal. Confirm with charities that they are collecting in your area.

# DATING AND ROMANCE SCAMS

**Many dating websites and chat rooms operate legitimately in the UK. However, individuals using them may try to scam you. Dating and romance scammers lower your defences by building an online relationship with you. Many people, both men and women, have lost huge amounts of money to online dating scammers. Always consider your personal safety if you arrange to meet someone through a dating website.**

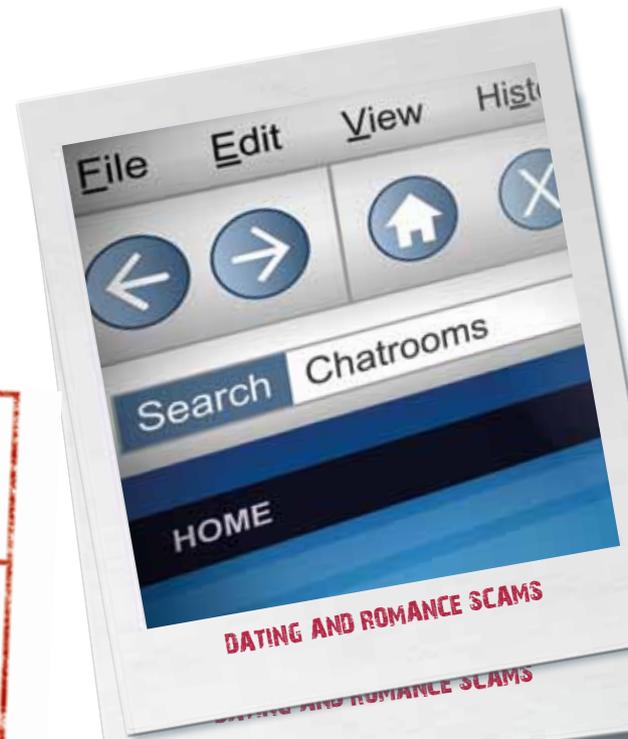
## What you should know

- ⚠ Be wary of giving out personal information on a website or chat room.
- ⚠ Scammers will quickly interact with you, often showing you glamorous photos of themselves and gaining your trust. But how do you know it is actually the person you are communicating online with?
- ⚠ Scammers will make conversation more personal to draw information from you, but will never really tell you much about themselves that can be checked or verified.
- ⚠ Scammers will normally try to steer you away from communicating on a legitimate dating website that could be monitored by staff. Their preference is to communicate via email, text and possibly phone, rather than through the dating website or chat room where you met.
- ⚠ A scammer will use a variety of scenarios to target your emotions and get you to part with your money (e.g. they have an ill relative or they are stranded in a country they don't want to be in and need money). THESE ARE SCAMS.
- ⚠ Never send money abroad, to a person you have never met or to anyone you don't actually know and trust.
- ⚠ Scammers will sometimes tell you to keep your online relationship a secret. Never agree to this. This is a ploy to get you not to tell your family and friends who will see the scam for exactly what it is.

**For reporting advice  
please see pages 36 and 37.**

## BIG SCAMS

<b>REMEMBER</b>	Check website email addresses carefully. Scammers can use illegitimate sites with similar addresses to legitimate ones.
<b>CAUTION</b>	Never send money, give personal information or bank details to a person you have never met. Always seek advice.
<b>THINK</b>	Always consider your personal safety if you arrange to meet someone through a dating website.
<b>INVESTIGATE</b>	How can you confirm the identity of the person you are chatting to online? Don't be afraid to ask questions and carry out checks.



# BANKING AND PAYMENT CARD SCAMS

**Protecting your card details is vital.**

**Card scams involve the use of stolen or counterfeit cards to make direct purchases or cash withdrawals and the use of stolen card details to buy items over the phone or via the Internet.**

## What you should know

### Phone

- ⚠️ Your bank and the police will NEVER ring you and tell you that they are coming to your home to collect your card, so never hand it over to anyone who comes to collect it. Should you receive a call like this put the phone down. THIS IS A SCAM.
- ⚠️ Depending on who you bank with, the security questions asked by the bank may vary (e.g. the last 4 digits of your account number or digits of your password) but your bank will NEVER ask you to authorise anything by entering your PIN into the telephone.

### ATM - Cash Machines

- ⚠️ NEVER share your PIN with anyone – the only time you should use your PIN is at a cash machine or when you use a chip and PIN machine in a shop.
- ⚠️ If there is anything unusual about the cash machine or there are signs of tampering, do not use it and report it to the bank as soon as possible.
- ⚠️ Do not get distracted. Be particularly cautious if ‘well-meaning’ strangers try to distract you or offer to help you and most importantly, discreetly put your money and card away before leaving the cash machine.
- ⚠️ Cover your PIN. Stand close to the machine and always use your free hand to cover the keypad as you enter your PIN to prevent any prying eyes or hidden cameras seeing your PIN.



## BANKING AND PAYMENT CARD SCAMS

### Banking

- ⚠ Check your statements regularly, including low value transactions. Notify your card company immediately if you suspect a fraud. Dispose of statements or slips which contain your card details carefully and securely by shredding or tearing your documents. This includes your cash machine receipts, mini statements or balance enquiries.
- ⚠ If you think someone is misusing your bank account details then report it to your bank.

**For reporting advice  
please see pages 36 and 37.**

## BIG SCAMS

### REMEMBER

NEVER share your PIN with anyone.

### CAUTION

Your bank or the police will NEVER ask to collect your card and your PIN.

### THINK

Check statements regularly to ensure they are correct.

### INVESTIGATE

If you suspect a fraud, contact your bank or the police immediately.



**Mobile phones have developed rapidly over the last few years and most now offer a huge range of functions. Smartphones are mini-computers so take all the precautions you would with your own computer at home.**

## What you should know

- ⚠️ If you use internet banking on your mobile, make sure you use an antivirus software so that it is protected.
- ⚠️ Text scams offering you money for an accident you may have had is often a ploy to obtain your personal details. Do not reply.
- ⚠️ You may receive a text message or advert encouraging you to enter a competition for a great prize. The scammers make money by charging extremely high rates for the messages sent from you to them. These could be as high as £2 per text message. Do not reply.
- ⚠️ With trivia scams, the first few questions will be very easy. This is meant to encourage you to keep playing. However, the last one or two questions you need to answer in order to claim your 'prize' could be very difficult or even impossible. Do not enter.
- ⚠️ If you try to claim your prize, you may have to call a premium rate number (that begins with 0906 for example). You may then have to listen to a long recorded message and there's unlikely to be a prize at the end of it. Do not phone back to claim.

**For reporting advice  
please see pages 36 and 37.**



**MOBILE PHONE SCAMS**



**MOBILE PHONE SCAMS**

**BIG SCAMS**

<b>REMEMBER</b>	Buy antivirus software for your Smartphone if you use it like a computer.
<b>CAUTION</b>	Do not reply to unsolicited text messages.
<b>THINK</b>	Is this a scam?
<b>INVESTIGATE</b>	Always conduct your own research before responding to any unsolicited text messages.

# HEALTH AND MEDICAL SCAMS

**Health and medical scams are commonplace. The scammers promise you miracle tablets and other medical cures that offer unbelievable results. Be wary of these advertisements and always seek medical advice before you purchase any product.**

## What you should know

- ⚠ A scammer may lead you to believe you will receive a product or service from them of a comparative or better quality for a lower price. This is a sales ploy to get you to buy their product. If it seems too good to be true it probably is.
- ⚠ Another type of scam involves fake online pharmacies offering drugs and medicines very cheaply or without prescription. Even if you do receive the product you order, there's no guarantee that they are the real thing.
- ⚠ These products are usually promoted by people who have no medical qualifications and exploit hopes for improved health.
- ⚠ 'Miracle' cure scams promise quick and easy remedies for serious conditions. At the very least you will be left out of pocket, but in some cases they may actually damage your health.
- ⚠ To help you identify a legitimate pharmacy, the Royal Pharmaceutical Society ([www.rpsgb.org.uk](http://www.rpsgb.org.uk)) has produced an internet pharmacy logo that acts as a visual aid for people who wish to buy medicine online. Only registered pharmacies providing professional services in the UK are entitled to display the logo.

**For reporting advice  
please see pages 36 and 37.**

# BIG SCAMS

**INSTANT WEIGHT LOSS!**

Try the most powerful weight loss formula



**HEALTH AND MEDICAL SCAMS**

## REMEMBER

These so called 'cure' products may not be the real thing and in some cases can damage your health.

## CAUTION

NEVER buy medicines, or any other treatments without seeking advice from a health care professional.

## THINK

Ask yourself: is the promise or offer too good to be true?

## INVESTIGATE

If you are being sold a product, check the company is reputable prior to purchase.

**Many internet scams take place without the victim even noticing. Ensure that you have antivirus software and a firewall installed on your computer and keep it up to date. If you are aware of the following precautions and apply common sense then you should be able to prevent yourself from becoming a victim.**

## What you should know

- ⚠ Scammers can use the internet to promote fraud through unsolicited or junk emails known as spam. Delete the email otherwise the scammer will continue to send you more and more emails from lots of different addresses.
- ⚠ Any email you receive that comes from an unknown sender is likely to be spam if it is not actually addressed to you and promises you some gain.
- ⚠ If you receive an email from someone you know but it is not the usual sort of message you get from them and it has an attachment DO NOT open the attachment. Speak to the person who is supposed to have sent it first before you reply. (The real sender may have infected it with a virus and forwarded it through their address book).
- ⚠ Online market places can be a lot of fun and can save you money but they are also used by scammers. Scammers will try to steer you away from online sites and request that you use unusual payment methods e.g. money transfer agents or Emoney (digital equivalent of cash, stored on an electronic device). This can also be stored on and used via mobile phones or in a payment account on the internet.
- ⚠ Scammers may claim that the buyer has pulled out of the auction you were bidding on and then offer the item to you. Once your money has gone to them you are unlikely to hear from them again and the auction site will not be able to help you.

## BIG SCAMS

<b>REMEMBER</b>	Delete all messages without reading them if they are from somebody you do not know. If you open it by mistake and it has an attachment, do not open that attachment. It may be a virus.
<b>CAUTION</b>	Don't reply to spam emails even to unsubscribe, and do not click on any links or call any telephone number listed in a spam email. Ensure you have antivirus software or see a computer specialist.
<b>THINK</b>	Never buy any item from a bidder with a poor rating. Be wary of any request to use an unusual payment method.
<b>INVESTIGATE</b>	Make sure the sites are genuine as some business websites can be copied, cloned or redirected.

⚠ The most common scams at the moment are for concert and event tickets, apartments, residential and holiday lettings, dating and romance scams and vehicles for sale or hire (especially if hire vehicles are to be delivered to you). Adverts and websites can be very sophisticated so do some research to ensure everything makes sense. Consider your personal safety when meeting anyone over the internet.



For reporting advice  
please see pages 36 and 37.

# PSYCHIC AND CLAIRVOYANT SCAMS

Psychic and clairvoyant scams happen when a scammer approaches you to tell you they have seen something either amazing or unpleasant in your future. They ask for money in order to supply you with the information.

## What you should know

- ⚠️ The psychic or clairvoyant scammer can approach you by email, post, phone or even face-to-face. They may try to convince you that they are genuine by telling you something about yourself.
- ⚠️ They may tell you that you are in some kind of trouble, but can offer you a solution in return for payment. They may claim to be able to give you winning lottery numbers or offer to remove a curse but will usually ask for an administration fee for their services.
- ⚠️ Psychic scams can also be used to set you up to fall for a lottery scam. If a psychic gives you a list of lucky lottery numbers, don't be surprised if you receive a letter soon afterwards telling you that you've just won a lottery you've never heard of and do not remember entering.  
THIS IS ALL PART OF THE SCAM.
- ⚠️ Scammers will often say you mustn't tell anyone else about your 'good news' such as a windfall as this will break your chances of winning. In fact this is a ploy to build trust and create a relationship in which you can be manipulated as you feel unable to turn to family and friends for advice.

**BE SUSPICIOUS**

**For reporting advice  
please see pages 36 and 37.**

## BIG SCAMS

### REMEMBER

Psychic and clairvoyant scams prey on your inquiring mind.

### CAUTION

Never give personal information to a psychic or clairvoyant.

### THINK

Carefully consider any advice given to you by a 'psychic.'

### INVESTIGATE

Check whether there is any proof to support the psychic's claims.



PSYCHIC AND CLAIRVOYANT SCAMS

# FREQUENT SCAMMING TOOLS

**Scammers often use one or more of the following to help them commit fraud and hide their true identity.**

## **Money Transfer Agents**

Using a money transfer agent is a way to send money to people that you know and trust. Money transfer agents offer fast, convenient and reliable options for customers to send and receive money worldwide.

However, they are often used by scammers in order to commit many types of fraud such as advance fee, identity theft, investments and mass market fraud to name a few.

**WHILST THE SENDER OF THE MONEY HAS TO PRODUCE IDENTITY DOCUMENTS, THOSE THAT COLLECT THE MONEY DO NOT.** This is why scammers will often try to get you to send them money using a money transfer agent. This method enables them to hide their identity.

## **You should:**

- ⚠ Never let a scammer educate you on how a money transfer service works - only take advice from the money transfer agent.
- ⚠ Read the warnings on money transfer documents. The information is there to protect you.
- ⚠ Do not pay for items bought online, including auction sites using a money transfer agent. Money transfer agents are not responsible for the satisfactory receipt of goods or services paid for by means of a money transfer.
- ⚠ Never share details of a money transfer with anyone else to prove the availability of funds. Doing so may enable the money transfer to be paid to that third party. This is known as a 'Proof of Funds' fraud.



## Virtual Offices

A virtual office is an address where any person or business wishing to use an alternative address to their own can use office facilities, telephone answering services or a postal address.

You might think you are dealing with a well established, professional individual or business with a prestigious address. However, the reality can be very different.

The majority of businesses using 'virtual offices' are honest and legitimate. However, scammers often use a virtual office address instead of their own in order to receive mail and conduct business using false ID to obtain the virtual office facilities.

If you see a website or an advert for a website that has a telephone number and address on it, be aware that the address could well be a virtual office address. Victims of many scams have been known to visit the address shown on a fraudulent website or on a letter in order to remonstrate and try to get back the money they have lost.

They are often surprised and dismayed to find that the office was a virtual office, used by a scammer who has provided the virtual office owner with false ID and that now there is no trace of the scammer.

Additionally a scammer may unscrupulously use a virtual office address without the virtual office owner's knowledge or permission. This is known as 'squatting.'



### Telephone Numbers

A handful of telecommunications companies are able to provide non-geographical telephone numbers (e.g. 0800 or 0845 numbers and premium rate numbers) to businesses or individuals. Depending on the type of service paid for, the customer does not have to provide identification. Scammers will often use these numbers and have them diverted to unregistered pay-as-you go mobile phone numbers or to a separate telephone answering service. You should not rely on the appearance of a telephone number to tell you what sort of number it is. For example '0208' is usually a London number and '07952' a UK mobile number. However, telephone numbers can be purchased by scammers to trick you into believing they are legitimate and based where you think they are. Always be cautious when speaking to people you do not know on the telephone.

Be aware that if the scammer gives out a telephone number, that phone number cannot always be traced and the user identified.

Be aware that if a scammer has paid for things to look legitimate – such as a prestigious address or free phone business number, then they may have paid for these items with compromised or stolen card details and therefore may not be identifiable.

Be aware that whilst banks are normally good at ensuring their customers are who they say they are, scammers can and do open up bank accounts using false details.



# FRAUD IS NOT A VICTIMLESS CRIME

## Scams DO happen

### Scam Mail - Think Jessica

Jessica received a very exciting letter that looked important and told her that if she sent a small fee it would release a large cheque that she had won in a competition. She quickly sent off the fee. On the claim form she put down all her personal details.

Unfortunately the letter was her first scam letter. When family members realised what she had done they tried to explain that she had fallen for a scam. But Jessica had never heard about scam mail and refused to believe what they said. Of course no money arrived, but the amount of what appeared to Jessica to be fantastic mail started to increase.

Unbeknown to her, the scammers who sent that first scam letter had put her name on a 'suckers list' and were selling her details to other criminals all over the world.

Jessica still refused to believe that her good news mail was only worthless pieces of paper designed by criminals, to make her part with her cash.

As the weeks turned into months the amount of scam mail she was receiving increased. Around 30 letters a day were arriving from all over the world that had things like 'Guaranteed Winner', 'Time Sensitive Document', 'Reply Immediately To Release Your Award' and various other slogans and logos plastered all over them.

Jessica was soon sending nearly all of her pension each week to keep up with the scammer's demands. So-called clairvoyants had also jumped on the bandwagon and were pretending to be her friends. To read more, see [www.thinkjessica.com](http://www.thinkjessica.com).



**SCAMS DO HAPPEN:  
THINK JESSICA**

**SCAMS DO HAPPEN:  
ROMANCE SCAM**

**Romance Scam**

A 60-year-old lady was scammed out of £60,000 in two months after joining an online dating site and befriending a man. Over the following weeks they developed a close relationship via emails and phone calls.

The man portrayed himself to be a successful Dutch businessman who earned his living supplying and fitting computers. He told her his partner had died and said he was estranged from family and friends. He said he had moved to the UK a year ago bringing his young daughter with him.

He claimed that while abroad on business, his daughter had been injured in a hit and run accident and required £9,600 for an operation in hospital. He did not ask for the money directly but claimed to have borrowed so much from the bank and that he had no-one else to turn to for help. He very subtly and cleverly manipulated her into taking a position of responsibility for his daughter's welfare. She wrestled with her conscience and whilst she did not want to give her hard-earned money to a

stranger, she did not want to leave a child to fend for herself. She wanted to pay the hospital directly but was told that they needed cash in advance. Having verified this online, she arranged money transfers.

Then the man said he needed £44,500 for his business and then further money for his accommodation and transport home. She repeatedly told him that she could not help and suggested other places to try, but with no success. He told her it was his responsibility to sort the money but claimed he had nowhere else to go. She perceived him to be a kind and gentle man, if naive about the practicalities of overseas business. He talked much of the times they would soon be able to spend together getting to know one another away from such difficulties.

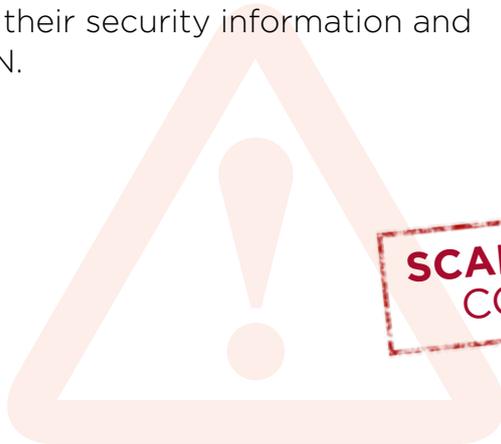
He asked her to meet his return flight at Birmingham airport so they could go to the bank together to return her money. Having received almost £60,000 in cash, he failed to arrive at the airport. She immediately reported her story to the police.

## Courier Scam

A 65-year-old man was scammed out of £12,000 as a result of a courier scam. The scammers purchased the use of an '0845' number and then contacted potential victims, details of whom they had obtained and researched on the internet. On phoning the victim they stated they were from a bank. They left an '0845' number with the victim to try and make their call look more legitimate. The victim contacted what they thought was their bank on the 0845 number supplied which was in fact diverted to the scammer's mobile phone. The scammer had sufficient details about the victim to build up trust. During the conversation the scammer cleverly managed to get the victim to divulge their security information and their PIN.

The scammer then persuaded the victim that their account was at risk and that they would dispatch a courier to collect the cards and take them to 'the bank' for examination. An unsuspecting courier was booked online by a scammer using stolen credit card data. The scammer then tracked the package containing the credit cards to a delivery address. The scammer took possession of the package from the courier. Once in their possession they checked the balance of the victim's account at an ATM and then bought high value goods to sell on to obtain cash.

This kind of scam is becoming more prevalent so be aware.



**SCAMS DO HAPPEN:  
COURIER SCAM**

# HANDY HINTS TO PROTECT YOURSELF

## Protect your identity

- ⚠️ Only give out your personal details when absolutely necessary and when you trust the person you are talking to.
- ⚠️ Destroy personal information. Make sure you shred all documents, old credit and debit cards and anything else with personal details on.
- ⚠️ Treat personal details like you would money. Don't leave them lying around for others to see and take.
- ⚠️ Be wary of who you give your personal details to in the street (e.g. charities, products, competitions etc). Do not sign up for anything until you have researched the company or charity.

## Money matters

- ⚠️ Never send money to anyone you don't know.
- ⚠️ Do not send any money or pay fees to claim prizes or lottery winnings.
- ⚠️ Jobs asking you to simply use your own bank account to transfer money for somebody could be a front for money laundering activity. Money laundering is a serious criminal offence and can carry a prison sentence of up to ten years.
- ⚠️ Avoid transferring or sending any refunds or overpayments back to anyone you do not know.

**YOUR PERSONAL  
INFORMATION IS  
VALUABLE:  
BE VIGILANT IN  
PROTECTING IT.**



## The face-to-face approach

- ⚠ If anyone comes to your door, make sure you ask for identification. You DO NOT have to let them in and they must leave if you tell them to.
- ⚠ Before you decide to pay any money, if you are interested in what a door-to-door salesman is offering, take time to find out about their business and their offer.



## Telephone business

- ⚠ If you receive a phone call from someone you don't know, always ask for the name of the person you are speaking to and who they represent. Verify this information by calling the company's head office yourself.
- ⚠ Do not give out your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.
- ⚠ It is best not to respond to text messages or missed calls that come from numbers you do not recognise. Be especially wary of phone numbers you do not know. They may charge you higher rates if you answer them and can turn out to be very expensive.

### Email offers

- ⚠ Never reply to spam emails, even to stop them. Often this just serves to verify that the address is active to scammers. The best course of action is to delete any suspicious emails without opening them.
- ⚠ Legitimate banks and financial institutions will never ask you to click on a link in an email to access your account and will never ask you for your PIN number.
- ⚠ Never call a telephone number or trust any contact details in a spam email.

### Internet business

- ⚠ Install software that protects your computer from viruses and unwanted programs and make sure it is kept current. If you are unsure, seek the help of a computer professional.

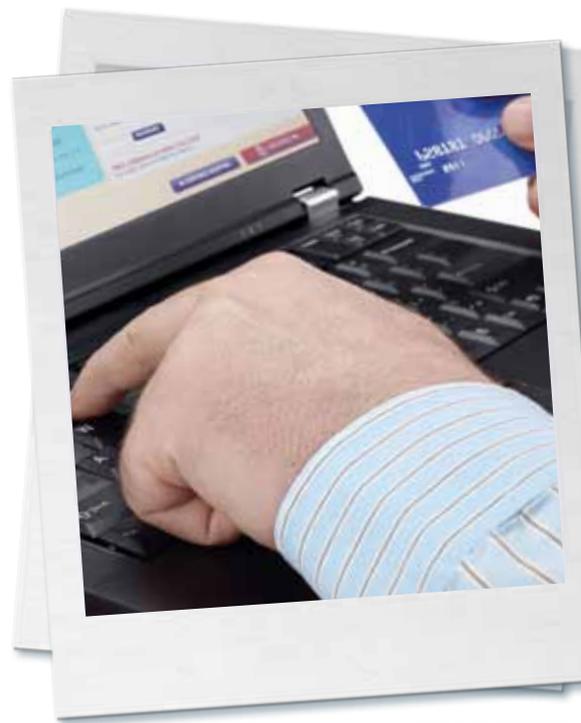
**BE SUSPICIOUS**



## General

Be suspicious and remember:

- ⚠ If it is too good to be true, it probably is.
- ⚠ Be aware of virtual offices, money transfer agents and other new and unusual methods of payment – e.g. Emoney. (Digital equivalent of cash, stored on an electronic device). This can also be stored on and used via mobile phones or in a payment account on the internet.
- ⚠ Be aware that if a scammer has paid for things to appear legitimate – such as a prestigious address or free phone business number, then they may have paid for these items with compromised or stolen card details.
- ⚠ Be aware that whilst banks are normally good at ensuring their customers are who they say they are, scammers can and do open up bank accounts using false details.
- ⚠ Be aware that scammers can be clever. They will have done their homework and will often know huge amounts of information about people they target. Often they are very organised and capable.
- ⚠ They will try to hide their true identity by using a variety of methods.



# WHAT TO DO IF YOU GET SCAMMED

## GET HELP AND REPORT A SCAM

If you think you have uncovered a scam or 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 urgent fraud matters

- a) **Where an immediate police response is required** – i.e. where the suspect is very near and/or the victim is at immediate risk – dial 999.
- b) **Where a police response is required**, e.g. for victim care or the suspect can be easily identified and located. Dial 101 or go into your local police station.



**REPORT A SCAM**

## Reporting non-urgent fraud matters

a) Where the suspect is not immediately identifiable or where the victim is not at immediate risk; Action Fraud is a national fraud reporting initiative. Non-urgent fraud matters should be reported to Action Fraud. Reports are then sent to the National Fraud Intelligence Bureau for analysis and possible investigation by the police. You can report either online or over the telephone.

### Action Fraud

Reporting online: [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

Telephone reporting: 0300 123 2040

**ActionFraud**  
Report Fraud & Internet Crime  
[actionfraud.police.uk](http://actionfraud.police.uk)

If you want advice from police when it is not an emergency, [dial 101](#).

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](tel:0800555111) or visit [www.crimestoppers-uk.org](http://www.crimestoppers-uk.org)

Crimestoppers is an independent charity.





### OTHER CONTACTS

#### Action on Elder Abuse

A national based charity (AEA) working to protect, and prevent the abuse of, vulnerable older adults.

Tel: 020 8835 9280

Helpline: 0808 808 8141 (Mon to Fri)

Web: [www.elderabuse.org.uk](http://www.elderabuse.org.uk)

---

#### Age UK

The new force combining Age Concern and Help the Aged; provides advice and information for people in later life through their Age UK advice line, publications and online.

Age UK Advice: 0800 169 6565

Web: [www.ageuk.org.uk](http://www.ageuk.org.uk)

---

#### Alzheimers Society

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

Tel: 0845 300 0336

Web: [www.alzheimers.org.uk](http://www.alzheimers.org.uk)

---

#### Citizens Advice Bureaux (CAB)

Citizens Advice Bureaux can help you solve your legal, money and other problems by providing free, independent and confidential advice.

For online information and to find your local CAB see [www.adviceguide.org.uk](http://www.adviceguide.org.uk) or look under C in the phone book.

Tel: 08444 111 444

Citizens Advice Consumer Helpline:  
08454 04 05 06.

Web: [www.citizensadvice.org.uk](http://www.citizensadvice.org.uk)

---

#### Financial Services Authority (FSA)

Provides information on how to find and choose a financial advisor and can confirm whether your advisor is authorised. It also produces a wide range of materials on finance-related matters.

Consumer Helpline: 0845 606 1234

Web: [www.fsa.gov.uk](http://www.fsa.gov.uk)

---

**JUST REMEMBER:  
IF IT SOUNDS TOO  
GOOD TO BE TRUE,  
IT PROBABLY IS.**

## **Insolvency Service**

The Insolvency Service is an Executive Agency of the Department of Business, Innovation and Skills (BIS). The Company Investigations team within the Insolvency Service has the power to investigate limited companies where information received suggests corporate abuse; this may include serious misconduct, fraud, scams or sharp practice in the way a company operates.

To complain about a limited company that is still trading:

**Tel: 0845 601 3546**

**Post: Intelligence Hub**

**Intelligence & Enforcement Directorate  
Investigation and Enforcement Services  
Insolvency Service**

**3rd Floor Cannon House  
18 Priory Queensway  
Birmingham B4 6FD**

**Email: [intelligence.live@insolvency.gsi.gov.uk](mailto:intelligence.live@insolvency.gsi.gov.uk)**

**Web: [www.bis.gov.uk/insolvency](http://www.bis.gov.uk/insolvency)**

---

## **Office of the Public Guardian (OPG)**

The OPG is responsible for protecting people who no longer have the capacity to make certain decisions themselves. It does this through:

- The supervision of Deputies appointed by the Court of Protection (CoP).
- The registration of Enduring Powers of Attorney (EPAs) and Lasting Powers of Attorney (LPAs).
- Maintaining a register of Deputies, Enduring Powers of Attorney and Lasting Powers of Attorney.
- Investigating allegations of abuse by Court appointed Deputies or Attorneys acting under a registered EPA or LPA.
- Policy ownership of the MCA and the Code.

**Office of the Public Guardian  
PO Box 16185 Birmingham B2 2WH  
Enquiry Line: 0300 456 0300**

---

## WHAT TO DO IF YOU GET SCAMMED

### SCIE

The Social Care Institute for Excellence (SCIE) improves the lives of people who use care services by sharing knowledge about what works. They are an independent charity working with adults, families and children's social care and social work services across the UK. They also work closely with related services such as health care and housing.

For general enquiries:

Tel: 020 7024 7650

Email: [info@scie.org.uk](mailto:info@scie.org.uk)

Web: [www.scie.org.uk](http://www.scie.org.uk)

---

### The Telephone Preference Service (TPS)

The TPS is a free service. It is the official central opt out register on which you can record your preference not to receive unsolicited sales or marketing calls. It is a legal requirement that all organisations (including charities, voluntary organisations and political parties) do not make such calls to numbers registered on the TPS unless they have your consent to do so.

To register free with the Telephone:

Preference Service Tel: 0800 398 893 or  
Web: [www.tpsonline.org.uk](http://www.tpsonline.org.uk)

---



## **The Mailing Preference Service (MPS)**

The MPS is a free service enabling consumers to have their names and home addresses in the UK removed from mailing lists used by the industry. It is actively supported by the Royal Mail, all directly involved trade associations and The Information Commissioners Office. It will take up to 4 months for the Service to have full effect although you should notice a reduction in mail during this period.

To Register for the Mail Preference Service:

**Tel:** 020 7291 3300 or

**Web:** [www.mpsonline.org.uk](http://www.mpsonline.org.uk)

---

## **The 'Opt Out' Services**

Companies may pass on your personal details to other companies unless you 'opt out'. Whether you are purchasing goods or obtaining a loyalty card you should carefully read all the terms and conditions to ensure your details are not forwarded without your consent.

The Royal Mail deliver letters addressed to 'The Occupier.' To 'opt out' of this service contact Royal Mail.

**Tel:** 08457 950 950

**Email:** [optout@royalmail.com](mailto:optout@royalmail.com)

---

## **Think Jessica**

If you are a victim of Mass Market Fraud then you can contact Think Jessica for advice.

**Email:** [advice@thinkjessica.com](mailto:advice@thinkjessica.com)

If you would like a Think Jessica information pack about scam mail (includes DVD). Please send a cheque or postal order for £5.00 (to cover production and postage).

**Think Jessica**

**PO Box 4244**

**Chesterfield S44 9AS**

---





## 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 for a follow-up scam.

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

### Report a scam

By reporting the scam to Action Fraud, Police or Trading Standards, 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. Any new scheme or initiative will quickly be targeted.

Finally, remember that this booklet does not contain all the answers but 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 scammer.

Be suspicious and remember if it is too good to be true it probably is!

An E-version of this document is available on our website  
<http://www.derbyshire.police.uk/scams>



**INTERNET SCAMS**



**DOOR-TO-DOOR SCAMS**



**MASS MARKET FRAUD - SCAM MAIL**



**INVESTMENT SCAMS**

**JUST REMEMBER:  
IF IT SOUNDS TOO  
GOOD TO BE TRUE,  
IT PROBABLY IS.**



**DATING AND ROMANCE SCAMS**



**IDENTITY FRAUD**



**BANKING AND PAYMENT CARD SCAMS**



**MOBILE PHONE SCAM**



**PSYCHIC AND CLAIRVOYANT SCAMS**

**BIG**  
SCAMS