# THE LITTLE BOOK OF BIG SCAMS

SECOND EDITION

Sussex Police
Serving Sussex
www.sussex.police.uk

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.

BIG SCAMS

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



BIG SCAMS

# INTRODUCTION

**Sussex Police is pleased to bring you the second edition of 'The Little Book of BIG Scams', reproduced by kind permission of The Metropolitan Police Service's Operation Stirling Team. The booklet was originally inspired by a publication, created by the Australian Competition and Consumer Commission.**

The second edition will increase your awareness of the new scams being used to con people out of their money. We have highlighted some scams that are on the increase, for example, courier fraud and insurance fraud. We want to teach you some easy steps that you can take to protect yourself (and others). It should be seen as a general guide to many of the scams currently operating in the UK.

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 victims and suspects. They can take a lot of resources to investigate and courts find it difficult to convict suspects because of the grey area that may appear to exist between dishonesty and sharp practice.

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

## Scams do not discriminate

Scams target people of all backgrounds, ages and income levels. Sussex Police has seen the devastating effects they can have on people and their families. One of the best ways to fight them is to 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).

## Protect Yourself

If you want to stay on top of scams and up to date about crime prevention advice, visit the Sussex Police website at www.sussex.police.uk

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

# 10 GOLDEN RULES

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

1. **Be suspicious of all 'Too good to be true' offers and deals. There are no guaranteed get-rich-quick schemes.**
2. **Do not agree to offers or deals immediately. 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/individual.**
4. **Never send money to anyone you do not know or trust (whether in the UK or abroad) or use methods of payment that you are not comfortable with.**
5. **Never give banking or personal details to anyone you do not know or trust. This information is valuable. Make sure you protect it.**
6. **Always log on to a website directly rather than clicking on links provided in an email.**
7. **Do not rely solely on glowing testimonials: find solid independent evidence of a company's success.**
8. **Always get independent/legal advice if an offer involves money, time or commitment.**
9. **If you spot a scam or have been scammed, report it and get help. Contact ActionFraud on 0300 123 2040 or online at actionfraud.org.uk Contact the Police if the suspect is known or still in the area.**
10. **Do not be embarrassed to report a scam. Because the scammers are cunning and clever there is no shame in being deceived. By reporting you will make it more difficult for them to deceive others.**



BIG SCAMS

# IDENTITY FRAUD

**Identity Fraud is often quoted as 'Britain's fastest growing crime.' It involves the misuse of an individual's personal details in order to commit crime. These personal details are very valuable. They 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


## 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:

- ⚠ Be extremely wary of unsolicited phone calls, letters and emails pretending to be from your bank, or other financial institution asking you to confirm your personal details, passwords and security numbers.
- ⚠ Regularly check and chase up statements that are not delivered when expected.
- ⚠ Dispose of anything containing your personal details by using a cross cut (confetti) shredder or tearing up into small pieces.
- ⚠ 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.
- ⚠ If you think someone is misusing your bank account details then report it to your bank.

## Protecting your Phones:

- ⚠ Never reply to unsolicited texts, e.g. texts referring to accident claims even to get them stopped. Simply delete them.
- ⚠ 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.

## 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.
- ⚠ 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 your 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.


**YOUR PERSONAL INFORMATION IS VALUABLE:** TAKE ACTION TO PROTECT IT.

BIG SCAMS

# COURIER FRAUD

**Courier frauds are becoming more prevalent and sophisticated. Usually the elderly are targeted. Scammers will telephone a potential victim purporting to be from their bank, from the police or other law enforcement authority. They then dupe the person into revealing their PIN and handing over their debit or credit card.**

## What you should know

- A scammer rings you, claiming to be from your Bank or the Police, saying a fraudulent payment has been spotted on your card and this needs resolving, or that someone has been arrested using your details and cards.
- You may be asked to ring back using the phone number on the back of your card. This further convinces you that the call is genuine. However, the scammer keeps the line open at their end so, when you make the call, you are unknowingly connected straight back to them or their friends.
- They will ask you for your PIN number or sometimes ask you to key it into your phone's handset. YOU SHOULD NEVER GIVE YOUR PIN TO ANYONE IN ANY WAY.
- The scammer then sends a courier or taxi to pick up your card from your home. It is possible the driver does not know they are being used as part of the scam.
- Once they have your card and PIN the scammer can then spend your money.
- There are many variations to this scam, one of which is where the scammer requests you to assist in a police investigation by asking you to go to your bank, withdraw a large sum of cash and take this home. Another is where you may be told there is a corrupt member of staff within your bank and the police need your help to identify them by withdrawing a large sum of your money with the purpose of the money being marked by police or the bank and placed back into the banking system. They say this will help them identify the corrupt person. You may be told not to speak to the bank about the investigation when you withdraw your cash as this may alert the criminal. You will then be asked to hand this to a courier or taxi driver and it will ultimately end up with the scammer. You may also be asked to purchase an expensive watch or other expensive items and hand this to the taxi driver.
- If you receive a call like this, hang up the phone. In order to clear your line from the scammer, wait at least 5 minutes before making any calls. DO NOT hand over any money or items purchased as a result of this type of phone call.

For reporting advice please see pages 37 and 38


BIG SCAMS

| | |
|---|---|
| REMEMBER | Your bank or the police will NEVER ask for your PIN, your bank card or to withdraw money. |
| CAUTION | NEVER share your PIN with anyone – the only times you should use your PIN is at a cash machine or when you use a shop's chip and PIN machine. |
| THINK | NEVER hand your bank card or any goods you have purchased as a result of a phone call to anyone who comes to your front door. |
| INVESTIGATE | If you think you have been the victim of this scam, call police. |

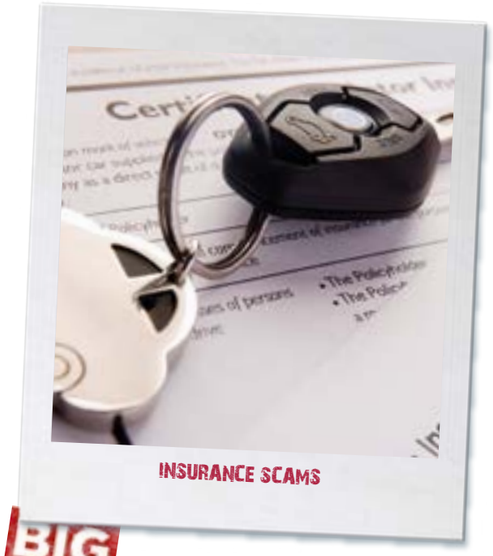
BIG SCAMS

# INSURANCE SCAMS

**Insurance fraud is on the increase and can leave you significantly out of pocket. According to the Insurance Fraud Bureau fraudulent claims cost £1.2 million a year, adding, on average, £50 to the annual costs individual policyholders face. Make sure if you have an accident, you obtain as much evidence at the time of the incident as possible and always obtain vehicle insurance directly through a reputable company.**

## What you should know

- ⚠ You may become involved in an accident, your fault or otherwise, where the other party is injured or significant damage is caused to their vehicle.
- ⚠ They may want to claim from you (through your insurer), but how genuine are they?
- ⚠ They may be part of a group trying to scam you and your insurers out of money. Known as 'Crash for Cash' they purposely cause an accident and fake an injury with the intention of getting a big pay out from you. This money then goes on to fund other criminal activities.
- ⚠ If police do not become involved, try and obtain as much evidence of the accident as possible, e.g. pictures of the damage.
- ⚠ Scammers also operate through websites or advertisements offering cheap insurance. This is known as 'Ghost broking'.
- ⚠ They target people on a budget and communities where English is not the first language.
- ⚠ Once you have agreed the terms and conditions, they will issue you with a fictitious policy which will be significantly cheaper than one you would have been quoted by the legitimate insurer. Remember – if it sounds too good to be true, it probably is!
- ⚠ In some cases, the scammer will apply to a genuine insurer on your behalf but will alter the details to get the lowest possible price. You may have agreed to these alterations, but you may also be totally unaware you are being scammed.
- ⚠ You not only lose your money but you may find yourself uninsured on your vehicle and may only discover this when you have a genuine accident.


For reporting advice please see pages 37 and 38

BIG SCAMS

| | |
|---|---|
| REMEMBER | If it sounds too good to be true, it probably is! |
| CAUTION | When it comes to insurance, always go through a reputable insurance company. |
| THINK | Am I being scammed? |
| INVESTIGATE | Obtain as much evidence as possible when you have an accident. |

BIG SCAMS

# 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. Often, victims of this particular scam are the elderly and vulnerable. There is a huge range and variety of mass market mail, some of which will be obviously fraudulent and others that will not. Whatever the case, you should always be wary of what you reply to.**

## 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 a single response 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. Even if you receive a prize it may not be what was promised to you.

⚠ Psychic and Clairvoyant 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.




For reporting advice please see pages 37 and 38

⚠ 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. Another marketing technique is to offer a share of a cash prize but to win you must place an order for goods that in fact are not value for money.

⚠ Be wary when sending money to and receiving money from someone you do not know and trust. This may be a ploy by a scammer to get you to pass money through your bank account that could be money stolen from someone else's account. Technically you will be money laundering and become what's known as a 'Money Mule'. This can carry a prison sentence if convicted so be wary and take action to protect yourself.

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. |

BIG SCAMS

# INVESTMENT SCAMS

**Investments where fraud is commonplace are land, wine, carbon credits, gold and jewels as well as stocks and shares. An up and coming investment scam involves the selling of rare earth metals. Many people have lost their entire life savings to investment scammers. Don't let it be you!**

## 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, including checking with Financial Conduct Authority (FCA) to see if they are a registered company.
- ⚠ Be wary of companies trying to recover your money from lost investments on your behalf for a 'one off' fee. This may be another scam trying to con you out of even more money.



BIG SCAMS

| | |
|---|---|
| REMEMBER | Do not respond to callers trying to sell you investments. Simply hang up the telephone. |
| CAUTION | 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. |
| THINK | Exercise considerable caution when investing your money especially in land, carbon credits, wine, jewels etc. |
| INVESTIGATE | Always seek independent/legal advice before committing to any investment. |



For reporting advice please see pages 37 and 38

BIG SCAMS

# DOOR-TO-DOOR SCAMS

**Many legitimate businesses sell products door-to-door (windows, solar panels, cleaning products, home maintenance, tree surgeons 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 people 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.
- ⚠ If someone knocks at your front door claiming to be from a company, always check their identity. If you are not happy then do not let them into your home.

**BE SUSPICIOUS**

**For reporting advice please see pages 37 and 38**


BIG SCAMS

| | |
|---|---|
| REMEMBER | If someone knocks at your door, always examine and check their identification. |
| CAUTION | Never let anyone in your house unless they are someone you know and trust. |
| THINK | Don't immediately agree to any offer involving a significant amount of money, time or commitment. Seek independent/legal advice first. |
| INVESTIGATE | 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. |

BIG SCAMS

# 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? Answer: You don't!
- ⚠ Scammers will make conversation more personal to draw information from you, but will never 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 37 and 38



BIG SCAMS

| | |
|---|---|
| REMEMBER | Check website email addresses carefully. Scammers can use illegitimate sites with similar addresses to legitimate ones. |
| CAUTION | Never send money, give personal information or bank details to a person you have never met. |
| THINK | Always consider your personal safety if you arrange to meet someone through a dating website. |
| INVESTIGATE | 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. |


BIG SCAMS

# BANKING AND PAYMENT CARD SCAMS


For reporting advice please see pages 37 and 38

**Protecting your card details is vital.**

**Card scams involve the use of stolen or counterfeit cards to make direct purchases or cash withdrawals or 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 to verify your PIN, withdraw your cash, purchase high value goods or that they are coming to your home to collect these items, 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!

⚠ If you receive a call from your bank or the police, verify who the person is before handing over any personal details. You can do this by calling your bank (the number on the back of your card) or the police (101) on a DIFFERENT phone line. This can be a mobile phone or a phone owned by your family, friend's or a neighbour. If no other phone is available, wait AT LEAST 5 minutes to ensure your line is clear to make the phone call. This is because currently, scammers are able to keep phone lines open. Whilst you think you are making a new phone call, the line is still open to the scammer who pretends to be a different person from your bank or the police (*see page 7 for Courier fraud*).

⚠ 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.

⚠ 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 it.

⚠ 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.

⚠ If your card does not get returned to you once it has been put in the machine, immediately contact your card issuer to cancel your card whilst you are still at or near the machine. Ensure you have your issuer's 24 hour contact number in your mobile phone or in your wallet or purse.

### 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 have to destroy your bank card then make sure you cut through the card including the CHIP. You can also use a shredder to destroy them.

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. |

BIG SCAMS

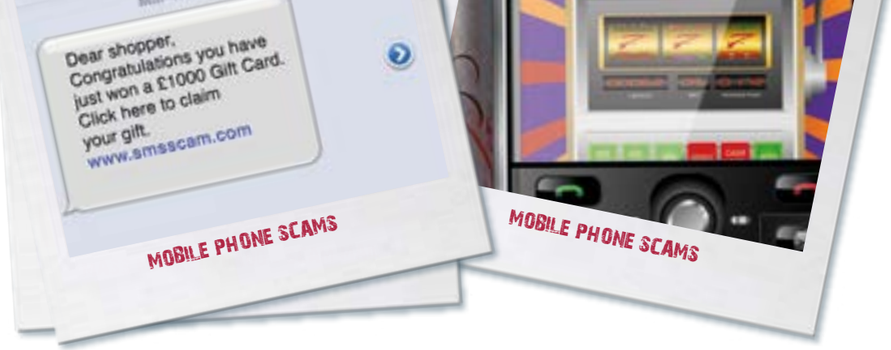
# MOBILE PHONE SCAMS

**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 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 – even to 'STOP' texts.
- 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 is unlikely to be a prize at the end of it. Do not phone back to claim.

For reporting advice please see pages 37 and 38




- 'SMiShing' occurs when a scammer sends you a text message asking you to provide personal and/or financial information. The message may appear to be from a legitimate company, like a mobile phone provider. Legitimate companies will not ask you to provide sensitive information by text. NEVER reply to these types of text messages.
- When using public Wi-Fi try to use commercial hotspot providers such as BT OpenZone or T-Mobile.
- Unless you are using a secure web page, do not send or receive private information when using public Wi-Fi.
- Be aware of who is around you when using a mobile device to go online.

BIG SCAMS

| | |
|---|---|
| REMEMBER | Buy antivirus software for your Smartphone if you use it like a computer. |
| CAUTION | Do not reply to unsolicited text messages. |
| THINK | Is this a product that I need? If it isn't then don't hand over money. |
| INVESTIGATE | If you are being sold a product, check that the company is who they say they are. |

BIG SCAMS

# 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.
- Be wary of newspaper adverts for rapid weight loss or teeth whitening treatments. Often you will be required to pay up front and in full for a series of treatments. However, the offices used may be hired by the scammer for a few days only. Don't be surprised if you do not receive the service you pay for. Scammers can and do disappear overnight with your money.
- To help you identify a legitimate pharmacy, the Royal Pharmaceutical Society (www.rpharms.com) 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 37 and 38

BIG SCAMS

# INTERNET SCAMS

**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.


- 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. Always consider your personal safety when meeting anyone over the internet.
- There are lots of ways scammers gain personal and/or financial information from victims – e.g. Phishing (unsolicited email purporting to be from a legitimate company requiring personal details), Vishing (voice over cold calling purporting to be from a legitimate company requiring personal details) and Spear Phishing (type of **phishing** scam that focuses on an individual or department within an organisation, addressed from someone within the company in a position of trust. They request information such as **login** IDs and **passwords**. This scam will often appear to be from a company's own internal unit and may ask employees to update their username and passwords. Once scammers get this data they can gain entry into secured networks. Another way is to ask users to click on a link, which deploys spyware that can take personal data from you). Never give your personal and /or financial details unless you know who you are giving them to.

BIG SCAMS

| | |
|---|---|
| REMEMBER | 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. |
| CAUTION | 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. |
| THINK | Never buy any item from a bidder with a poor rating. Be wary of any request to use an unusual payment method. |
| INVESTIGATE | Make sure the sites are genuine as some business websites can be copied, cloned or redirected. |

For reporting advice please see pages 37 and 38




BIG 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.

Be wary of individuals asking you for money upfront by using cash vouchers. Ensure you know who the individual is you are dealing with before providing them with any reference numbers they require to collect the money you have deposited.

## You should:

- ⚠ Never let a scammer educate you on how a money transfer service works – only take advice from the money transfer or cash voucher company.
- ⚠ 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 disappeared and left no trace other than a false ID.




## 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.

BIG SCAMS

# FRAUD IS NOT A VICTIMLESS CRIME

## Scams DO happen

### Health – Cancer cure scam

A local BBC consumer affairs program in Wales had been investigating a husband and wife who had been offering a treatment program in their home to cure cancer. The Medicines & Healthcare Products Regulatory Agency investigated the pair after the husband was previously imprisoned for using a similar device on children who had cancer. This time the victims, all of which were adult females, invited to the address, diagnosed with cancer and offered a treatment session(s) to cure them of a disease they did not have. The couple would 'cure' them by using a combination of rubs, pills and a device called an IFAS machine. This machine contained a number of glass instruments linked to an electrical current which produced a small current to the body. Some of the other treatments that were given were sexually motivated. In April 2012 the husband was sentenced to 8 years in prison and placed on the Sex Offenders Register. His wife was given a 6 month prison sentence and placed on the Sex Offenders Register.

### Health – Aids cure scam

This scam involved two individuals from West Africa who ran a website offering medical devices and supplementary medicine to cure Aids. All the victims involved were from the West African community. The scammer's website provided extremely well researched and detailed information on HIV & Aids. This was to deceive sufferers into believing the scammers were professional and legitimate. They offered a 'device' for over £125.00, which was no more than a cheap 'Tens' machine with added weights and connections. The sufferer was also committed to purchasing medicine for around £29.99, which was no more than flavoured gas purchased from fitness shop suppliers for £1. The Medicines & Healthcare Products Regulatory Agency were notified and carried out forensic testing on the machine and medicines supplied. The scammers were found guilty of fraud and received community service plus costs.

### Courier Scam

A 74 year old woman was scammed out of £5,000 as a result of a courier scam. The woman was contacted by the scammer claiming to be a police officer from the Metropolitan Police. He stated that there had been fraudulent activity on the victim's bank account in Poland and an undercover operation was going to be carried out at her bank in the local area. The woman was asked to provide the details of her debit and credit cards, PIN numbers and to withdraw £5,000 cash so this could be fingerprinted. She was told the money would be given back to her at a later date. The scammer called back the following day purporting to be another police officer from New Scotland Yard and gave her a police reference number. He asked her to package the cash and the cards separately and they would be collected in stages. She was told she would be updated once the packages had been received by the police. Within 2 days, both packages were collected by different couriers. On hearing nothing, the woman contacted the police and was told she was a victim of a scam and had lost her money and her cards.

This kind of scam is rapidly increasing so be aware.

# 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.

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

## 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.
- Responding to 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 fourteen years.
- Avoid transferring or sending any refunds or overpayments back to anyone you do not know.



## 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, before handing over any money.
- Contact your local Trading Standards if you are unsure about a trader that comes to your door.

## 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 on a different phone line in case the caller is holding the line open.
- Never 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.


## General

Be suspicious and remember:

- If it sounds 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 services 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, 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

In the Sussex Police area, all fraud should be reported to Action Fraud, however, where the victim is vulnerable or elderly, you may wish to contact Sussex Police directly by calling 101 or emailing 101@sussex.pnn.police.uk

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

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

REPORT A SCAM

### Unless

- ⚠ A crime is in progress or about to be.
- ⚠ 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, or dial 101 or go into 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

**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

**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

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

Tel: 0845 300 0336
Web: 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 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

**Financial Conduct Authority (FCA)**
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: 0800 111 6768
Web: www.fca.org.uk/consumers

## 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
Web: 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



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

## Royal Mail scam mail helpline

### What can I do about scam mail?

Scams can come to you by phone, email or post. There are many different types of scams, such as fake lotteries and prize draws, get-rich-quick schemes, bogus health cures, investment scams and pyramid selling, to name just a few. It's important to note there is a difference between scam mail and legitimate mail sent by companies to advertise lawful services or the sale of genuine goods. Scam mail is sent for the sole intention of obtaining money through deception and/or fraud.

Royal Mail is bound by the Universal Service Obligation and is required by law to deliver all mail entrusted to it. However, we are determined to do all we can to prevent scam mail entering the postal system with the help of our customers. We want to know about potentially fraudulent mail so we can work with the relevant authorities who can then investigate and take action.

### What to do

If you think you or a family member is receiving scam mail, you can report it to us.

If you have received items of mail you believe to be from fraudsters please send them to us, with a covering letter to:

Freepost
Scam Mail
PO Box 797
EXETER
EX1 9UN

You can also email us at scam.mail@royalmail.com or report your concerns by calling 08456 113 413. We will send you a scam mail report form for completion together with a prepaid addressed envelope in which to return the form with examples of the scam mail received.

### If you are moving home

To reduce the risk of identity fraud you should use Royal Mail's *Redirection* service to redirect mail from your old address to your new address for at least a year. If you hold power of attorney for somebody who you believe is a victim or vulnerable to being a victim of scam mail you can apply on their behalf for a Redirection of mail at a Post Office® branch or by post.

BE SUSPICIOUS

## 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
Web: www.scie.org.uk

## The Medicines and Healthcare Products Regulatory Agency

The role of the MHRA is to protect and improve the health of millions of people every day through the effective regulation of medicines and medical devices, underpinned by science and research. The MHRA operates one of the few enforcement functions within Europe dedicated to investigating offences against the Medicines and Medical Device regulations. It operates a full time intelligence unit, case referrals units for both medicines and devices and dedicated enforcement teams.

Tel: 0203 080 7701
Web: www.mhra.gov.uk
Medicines and Healthcare Products Regulatory Agency
151 Buckingham Palace Rd
London SW1W 9SZ

To report suspected non-compliant medical devices:
Email: devices.compliance@mhra.gsi.gov.uk

To report suspect medicines:
Email: casereferrals@mhra.gsi.gov.uk

To report suspected counterfeit products:
Email: counterfeit@mhra.gsi.gov.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: 0845 703 4599 or
Web: www.mpsonline.org.uk



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

## 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.

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

## 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 TPS:

Tel: 0845 070 0707 or
Web: www.tpsonline.org.uk

## Think Jessica

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

Email: 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 again.

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

### Report a scam

In the Sussex Police area, all fraud should be reported to Action Fraud, however, where the victim is vulnerable or elderly, you may wish to contact Sussex Police directly by calling 101 or emailing 101@sussex.pnn.police.uk

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 sounds too good to be true it probably is!

An E-version of this document is available on our website
**www.sussex.police.uk**

To request further information contact Sussex Police by emailing
101@sussex.pnn.police.uk
or by calling **101** on the phone.




**We would like to thank The Metropolitan Police Service's Operation Sterling Team and their partners for their time and effort in producing this booklet.**

Australian Competition and Consumer Commission
Financial Fraud Action UK
The Insolvency Service
The Medicines and Healthcare Products Regulatory Agency

Published by the Metropolitan Police Service


Published by the Metropolitan Police Service 