SCAMBUSTER

This document has been prepared using information from the Scambuster booklet issued by the defunct Office of Fair Trading and other information available online.

Contents

WATCH OUT!	2
PROTECT YOURSELF FROM SCAMS	2
COMMON SCAMS	3
ADVANCE FEE	3
CLAIRVOYANTS AND PSYCHICS	3
INVESTMENT OPPORTUNITIES	4
LOTTERIES	4
MIRACLE HEALTH CURES	5
ONLINE DATING	6
Phishing	6
PRIZE DRAWS AND SWEEPSTAKES	7
PYRAMID SELLING AND CHAIN GIFT SCHEMES	
WORK-FROM-HOME SCHEMES	8
OTHER SCAM TYPES	8
CUT THE IUNK	10

Watch out!

Scams are schemes to con you out of your money. They usually come by post, phone or email.

There are hundreds of scams – fake lotteries and prize draws, get-rich-quick schemes, bogus health cures, investment scams, pyramid selling. The list goes on.

Every year, three million people in the UK are victims of scams, often losing hundreds or even thousands of pounds. The scammers are clever and people from all walks of life get duped.

This booklet sets out varies types of scams and how to protect yourself. Scam examples used are fictional but based upon real examples.

Protect yourself from scams

Don't let the scammers con you. Follow these tips to avoid getting tricked out of your money.

Be sceptical

Beware of extravagant promises. Remember: If it sounds too good to be true, it probably is. Don't be afraid to bin it, delete it or hang up.

Take your time

Scammers don't like to give you time to think. They will try to pressure you into making a decision by telling you that if you don't act now, you'll miss out. Resist any pressure to make a decision right away. Consider asking a friend or family member for advice, or even an accountant or solicitor if big sums of money are involved.

Know who you're dealing with

Be suspicious if you're contacted out of the blue by someone you've never heard of. This is often a clear warning sign that it's a scam. And don't be fooled by official looking websites and marketing materials. Scammers are very good at making their scams look authentic.

Protect your financial information

Never give your bank account details and passwords to someone you don't know. Trustworthy firms will never contact you to ask for this information.

Cut junk mail and calls

Take some simple steps to cut the number of unsolicited offers you receive – see how on page 10.

Report or get advice on scams

To report fraud or get advice, consumers across the UK can visit www.actionfraud.org.uk or call <u>Action Fraud</u> on 0300 1232040 (textphone 0300 1232050) or forward scam emails to email@actionfraud.org.uk

Consumers in England, Wales and Scotland can contact <u>Consumer Direct</u> on 0845 4040506 or visit www.direct.gov.uk/consumer for advice on scams.

Consumers in Northern Ireland can contact <u>Consumerline</u> on 0300 1236262 or visit www.consumerline.org for advice and to report scams.

Common scams

Advance fee (This scam is sometimes called the '419 scam' or the 'Nigerian letter').

A letter or email offers you a huge payment if you can help get money out of a foreign country. The writer might claim to be a government official, an accountant or a lawyer. They will tell you that they need to transfer millions of dollars to the UK – perhaps because of some major event in their country such as a coup or natural disaster. You're promised a slice of that money for helping with the transfer. You may be asked for your bank details. The scammers then raid your bank account. Alternatively, you will be told to send an upfront fee. Either way, you never see a penny of the promised payment.

Protect yourself

- ➤ Just say no. These kinds of offers will always be a scam and you'll lose your money.
- Never give your bank details or passwords to people you don't know.

Could it be you?

Byron Hopkins from North Wales received an email claiming to be from the lawyer of a deposed politician in a war torn African country. The email said that the politician urgently needed to move \$10 million out of the country by transferring it to a UK bank. Byron was promised 10 per cent of the money – a million dollars – for his help. All he had to do was provide his bank account details.

The email stressed the importance of keeping the transaction confidential. It said that, if he told anyone about it, he would risk missing out on the enormous commission on offer.

Byron emailed back his bank account details and the scammers duly emptied his account. He lost more than £650.

* This example, and the others that follow, are fictional but based on actual cases.

Clairvoyants and psychics

A letter from a so-called psychic or clairvoyant promises to make predictions that will change your life forever – but first you have to pay a fee.

Sometimes these mailings are aggressive, saying something terrible will happen to you if you don't pay up. Or the scammers say they have seen wonderful things in your future, and request money for a full report. If you send money, you will get little or nothing back. And you are likely to be bombarded with further scam mailings. These kinds of letters are sent to tens of thousands of people to con them.

Protect yourself

- Don't be intimidated into replying. Bin it!
- Talk to someone.

Could it be you?

A 'clairvoyant' wrote to pensioner George Robson of north London to warn him that an angel had told her something terrible was going to happen to him. She said she would say an 'angel prayer' to protect George − as long as he sent her £19. He was frightened and sent off the money. Over the months that followed, George received many similar dire warnings and demands for payment. He ended up losing more than £150 before his grandson spotted that he'd been duped.

Investment opportunities

You're offered the chance to put money into things like shares, gemstones or fine wine. The promise is that these will rocket in value. In reality, what you are being offered is often over-priced, very risky and difficult to sell on.

Most of these so-called investments are run from overseas and may not be authorised by the UK's <u>Financial Services Authority</u>. As a result, there is almost no chance of getting your money back if things go wrong.

Protect yourself

- ➤ Be very sceptical about calls out of the blue from companies you don't know offering shares and other investments, especially if they're 'guaranteed' or 'risk-free'.
- > Get independent financial advice before making an investment.
- Never sign up to anything immediately or if you're told to keep the deal confidential.
- Make sure the firm is on the <u>Financial Services Authority</u> register of authorised firms by checking at www.fsa.gov.uk

Could it be you?

Paul Wood from Derbyshire lost almost £25,000 to a Spanish 'investment company' − even though he had 20 years of experience of investing in shares.

It started when he received a phone call out of the blue telling him about a new genetics company about to be floated on the US stock market. He was offered shares in the company at less than a fifth of their likely market value.

After sending off a cheque for £6,000, Paul started receiving monthly statements showing how his shares were shooting up in value. He ploughed more money into the shares as his confidence grew. He even bought his wife a new car.

It wasn't until a year later when he tried to sell his shares that he realised it was a scam. He couldn't get hold-of any of the people he had been dealing with. The companies were fronts and the shares were worthless.

Lotteries

Congratulations! A letter, phone call, text message or email tells you you've won a huge sum of money in a lottery – even though you haven't bought a ticket.

You're told that, to claim your winnings, you need to send money to cover 'processing' or 'administration' costs or taxes. You may also be asked for personal or financial information for 'identification'.

This is a scam. The scammers will take your money and you will get nothing in return. And if you send one payment they will contact you again and try to con you out of even more.

Protect yourself

- Ask yourself how you could win a lottery if you haven't bought a ticket.
- Remember that, if you have won something, you shouldn't have to pay anything to get your prize.
- Never reveal credit card or bank account details unless you're sure who you're dealing with.

Could it be you?

'Congratulations!' began the letter that arrived one morning for Brian Gregory from Coventry. Reading on, Brian was amazed to learn he'd won €1.2m in a Spanish lottery. It was a bit odd – he knew he hadn't bought a ticket. But the letter looked convincing – it was even signed by the President of the lottery company. And it was a life-changing amount of money.

Brian called the phone number on the letter right away. He was told that it really was true. There was just some paperwork to take care of. Before his winnings could be released, he simply had to make a payment by Western Union of £670. This was to cover things like a 'processing fee' and a 'tax'. Brian sent the money but of course never received the promised prize.

Never reveal credit card or bank details unless you're sure who you are dealing with.

Miracle health cures

You see an ad, website or email offering a 'miracle cure' or 'scientific breakthrough' that will cure a health problem such as arthritis, diabetes or cancer, or help you lose weight.

The seller will usually say there is only limited availability, and offer a 'no-risk, money-back guarantee' or a 'free trial'. There will probably be quotes from doctors and satisfied customers.

These claims are exaggerated to con you out of your money. It is highly unlikely that the medicines being offered will deliver the quick or miracle cure promised. They may even be harmful.

Protect yourself

- Be sceptical about health related claims. If it sounds too good to be true, it probably is.
- Consult a medical professional, such as your GP or NHS Direct, before buying any 'cure' by mail order or over the internet.

Could it be you?

After years of being overweight, Viv Hamilton from Exeter came across a website promoting a new berry that would help her slim down without exercise.

The site included lots of quotes from satisfied customers and before-and-after photos. It offered a free 30-day trial of the berry extract in pill form − she just needed to pay £3.95 postage. Viv entered her credit card details.

After 10 days, she received the trial pills. She took-them for a month, but they had no effect. Then more pills arrived. On her credit card statement, she saw she had been billed the initial £3.95 plus £75 for the next month's supply. She tried contacting the company to ask for a refund but her calls and emails went unanswered. She never got a penny back and had to cancel her card.

Online dating

You sign up to an online dating service and meet someone who sounds like the perfect match. You send messages to each other for a while until the person asks for some kind of financial help. Things the person might say before pleading for your money include:

- "I want to come and meet you but can't afford the flight."
- "I have been robbed."
- "I need urgent medical treatment."

You pay up to help your new friend – but he or she disappears, along with your cash.

Protect yourself

- Never send money to someone you don't know, however plausible they sound.
- ➤ Only use a reputable online dating or chat service and follow their safety tips.
- > Report any suspicions to the dating site.

Could it be you?

Having signed up to a popular online dating site, Wendy Groves met a man who sounded like her dream partner. He was a former soldier who now worked on container ships sailing between the UK and Asia.

After several months of sending increasingly affectionate messages, the man sent an email saying he'd been beaten and robbed while in port in Singapore and his ship had left without him. He asked Wendy to send him £600 by Western Union so he could afford to fly to the ship's next port of call.

Wendy sent the money that day. She never heard from the man again.

Phishing

You get an email that looks like it's from your bank. The message may ask you to 'update', 'validate', or 'confirm' your details. It will probably direct you to a website that looks just like your bank's site. It's all designed to trick you into revealing your personal information and passwords so the scammers can raid your account, run up bills or commit financial crimes in your name.

This is called phishing.

Protect vourself

- Remember: Although your bank may contact you by email, they will never ask you to confirm your user name or password by clicking on a link in an email and visiting a website.
- Forward suspected phishing emails to your bank and then delete them.
- Read the advice on www.banksafeonline.org.uk

Could it be you?

One evening, an email landed in Karen Rossiter's inbox from her bank. It asked her to update her account details 'as part of our commitment to protect the integrity of your account'.

She clicked on the link and was taken to a website that looked just like her bank's site. She typed in her account details including her customer number and password. She hit 'Send' and got a reassuring confirmation message.

Next time she signed into on line banking, she was horrified to see that her account had been emptied and she was almost £1,000 overdrawn.

Prize draws and sweepstakes

You find out that you've won a guaranteed prize in a prize draw or sweepstake. You just have to pay a 'processing' or 'administration' fee, or order a product, to get your prize.

You're told you have to respond quickly. You may also be asked to call a premium-rate phone number.

In many cases, you're paying simply to enter a prize draw or sweepstake with a very slim chance of winning. Anything you might 'win' is usually worth far less than what you've paid out. In other cases, the scammers simply take your money and you never hear from them again.

What's more, once you respond to one bogus promotion, your details will be sold to other scammers and you'll get even more scam mail.

Protect yourself

- Remember that, if you have won something, you shouldn't have to pay anything to get your prize.
- ➤ Don't dial a premium-rate number (beginning 090) unless you know how much you'll be charged and you or the person paying the bill are willing to pay.

Could it be you?

A letter out of the blue told Sylvie Townsend from Wiltshire that she'd won £15,000 in a sweepstake. She was told to imagine everything she could do with this 'guaranteed' prize. The letter urged her to respond right away to avoid missing out.

Sylvie was told to send an 'administration' fee of £15 to a PO Box address so that her prize could be released. She thought it was a small amount to pay for a chance of a big win so she sent off a cheque.

Her cheque was cashed, but she received nothing in return. And she was soon receiving dozens more scam mailings every week. It became very distressing.

Pyramid selling and chain gift schemes

You hear about a great new money-making venture. You agree to go to a presentation where you are told that after paying a joining fee, you can earn large amounts by recruiting new members to the scheme.

This is pyramid selling. In reality, only a tiny minority of those involved make money. Everyone else loses. Pyramid selling is illegal.

In a similar scam, you are offered an expensive gift. But first, you have to buy a low-value item. You get your high-value gift only if lots of new members sign up – and you have to recruit them. You're very unlikely ever to get the gift.

Protect yourself

- Avoid schemes that offer money or a gift based purely on signing up new members.
- > Don't agree to anything at high-pressure meetings or seminars.
- > Don't hand over any money or sign a contract to participate in any multi-level marketing plan until you've investigated it.

Could it be you?

Debbie Morris of Norfolk received an email from an old school friend about a scheme that promised 'You and your friends can enjoy wealth together'. Normally, she simply deleted dodgy-looking emails. But, as this one was from a friend, she thought she should at least look into it.

She agreed to go to a seminar. There, she was given a brochure and witnessed several people getting cheques for £12,000 after apparently having put up just £3,000. The organisers persuaded Debbie to sign up there and then.

Only afterwards did it sink in that she had to recruit 100 people to the scheme before she would make money. She felt too embarrassed to tell anyone and resigned herself to losing £3,000 – almost all her savings.

Work-from-home schemes

You see an ad in a newspaper, on a website or even on a lamppost offering work from home with the promise of fast cash for minimal effort.

When you reply to find out more, you learn that you have to pay an upfront fee to the organisers.

They will take your money and are unlikely to pay you for any work you do. Or you may find that there is no work on offer, only commission for getting other people to sign up.

Of course, there are some genuine work-from-home schemes. They will tell you in writing exactly what you will be expected to do, how much you will earn, and how and when you will be paid.

Protect yourself

- If you reply to a job ad and are asked for money in advance, walk away.
- ➤ Before signing up to a work-from-home scheme, do a web search on the company, and ask to speak to current workers.

Could it be you?

A flyer on a lamppost in Edinburgh city centre caught the eye of Maggie Ross. It promised substantial earnings for envelope-stuffing work she could do at home.

Maggie called the mobile number on the flyer. She gave her name and address and received a form and a request for a £45 registration fee. Maggie sent the money but all she got back was instructions for enlisting other people on the scheme. She realised she had been tricked.

Maggie tried calling the original phone number to demand a refund, but the number was out of action.

Other scam types

Career opportunities

You're tempted with an opportunity to launch an exciting new career – for instance, as an author, a model or an inventor, or perhaps as a mystery shopper. All you have to do to guarantee success is to pay an upfront fee for training, study aids or materials. You might be asked to sign a credit agreement, which can't be cancelled.

Unfortunately, you get little or nothing in return.

Chain letters

You receive a letter with a list of names and addresses. It invites you to send a small sum, perhaps £10, to the person at the top of the list and then add your own name to the list photocopy it and send it out to, say, 200 people. The letter says you're guaranteed a return of thousands of pounds. In fact, it's almost certain you'll never see a penny. This scam operates like pyramid selling − see page 7.

Cheque overpayment

Someone responds to your ad or eBay posting with an offer to pay by cheque. The buyer sends a cheque for more than the purchase price and asks you to return the difference. Usually, the cheque is a fake, but good enough to fool bank tellers. You transfer some money back to the buyer, but soon your bank contacts you to say the buyer's cheque has bounced. There's no way to recover the money you've lost.

Pay-in-advance credit

A company claims you've 'pre-qualified' for a guaranteed loan or credit card – even if you have a bad credit history. You just have to pay a processing fee.

This fee is non-refundable and may be several hundred pounds. In reality, a pre-qualified offer only means you've been selected to apply. You can still be turned down. If so, you lose your processing fee and end up with no loan or credit card.

Legitimate lenders never 'guarantee' a card or loan before you apply.

Premium-rate prize draws

You're offered an exciting prize or reward. To claim it, you have to phone a premium-rate number (starting 090). The message you hear when you call tricks you into staying on the line. The longer the call, the more the scammers make from you. And your prize or reward is unlikely to turn up or will be worth much less than the cost of the call.

Legitimate companies tell you up front how much their premium-rate lines cost per minute.

Property rentals

You want to rent a property. Before checking your references, the landlord asks for a deposit – usually a month's rent – and gets you to sign a short contract. The contract states that, if the references are unsatisfactory, your deposit will be paid back – minus a fee for checking the references.

The landlord contacts you to say your references are unsatisfactory, no matter how good they really are. You're told you can only have a small portion of your deposit back because of the expense incurred checking references. You may end up losing hundreds of pounds.

Racing tipsters

You're offered horse racing tips guaranteed to make you a fortune. All you have to do is pay a fee, follow the tips and watch your winnings roll in. Usually, the offer will come from a 'racing insider' who, owing to his gambling success, has been banned from placing bets. After handing over your cash, you find the tips are poor or non-existent.

Ticketing

A website promises tickets to a sports or music event when it's already sold out or when tickets haven't yet gone on sale. You pay, but never see the tickets.

Of course, there are legitimate ticketing websites. A telltale sign of a scam is if the company doesn't give a full UK street address and landline phone number.

Postal/Parcel scam

A card is posted through your door from a company called PDS (Parcel Delivery Service) suggesting that they were unable to deliver a parcel and that you need to contact them on 0906 6611911 (a Premium rate number). Do NOT call this number, as this is a mail scam originating from Belize. If you call the number and you start to hear a recorded message you will already have been billed over £300 for the phone call.

If you receive a card with these details, then please contact Royal Mail Fraud on 020 7239 6655.

Pension/State Pension

You are offered advice concerning a pension from your employer or the state – specifically about investing any lump sum you may be due. 99% of these are bogus as they are only interested in stealing all your money.

Impersonation

A scam where a telephone caller claims to be calling from a court and tells you that you have only a few days to avoid attending a court hearing and a fine of £5000, but you can avoid this by making a smaller payment to them immediately over the phone. This is *not* how the UK courts operate.

If a real court hearing was to take place you would be informed formally in writing and given sufficient notice for you to obtain advice before attending. Her Majesty's Courts & Tribunals Service would never make unsolicited phone calls, demand money in advance to prevent a court hearing from taking place, or seek payment through cash vouchers bought in local shops.

A scam involving a telephone call from someone claiming to be from the Ministry of Justice or other government department. These callers usually have strong foreign accents and use fake anglicised names. Consumers are typically told that they are eligible to receive payments such as the repayment of bank charges or tax, compensation for mis-sold payment protection insurance (PPI), or other debts.

If you receive a suspicious call from the Police, demand that they send a uniformed police officer to see you.

Cut the junk

You can take some simple steps to cut the number of unsolicited offers you receive by post, phone and email. This will make it harder for the scammers to reach you. And it will give you the confidence to treat any offers you do receive with extra caution.

Mailings

Reduce the number of unsolicited letters and other mailings you get by registering for free with the <u>Mailing Preference Service</u> at www.mpsonline.org.uk or by phoning 0845 7034599.

Telephone calls

Reduce the number of unsolicited phone calls you get by registering your phone number for free with the <u>Telephone Preference Service</u> at www.tpsonline.org.uk or by phoning 0845 0700707.

You could also ask your telephone company to block callers who withhold their number. They can even bar you from making calls to premium-rate 090 numbers (some phone companies charge for doing this).

Text/SMS messages

Reduce the number of unsolicited phone calls and texts you get on your mobile phone by registering your number for free with the <u>Telephone Preference Service</u> at www.tpsonline.org.uk or by phoning 0845 0700707. If you receive a text/SMS service you don't want, reply with the word STOP. The service should end immediately.

For more advice or to make a complaint, contact your mobile network or <u>PhonepayPlus</u>, the regulator of services paid for through your mobile phone bill, on 0800 500212 or at www.phonepayplus.org.uk

Email

Reduce the number of unsolicited emails you get by installing anti-spam software and a firewall on your computer. And then keep them up-to-date. For advice, go to www.getsafeonline.org.

Surveys

Although not strictly always scams, taking part in telephone surveys only serves to allow sellers of products to target you in future more accurately with things they believe they can sell you. This results in more phone calls to you.

For more tips and to report scams you've spotted, go to www.consumerdirect.gov.uk/scams.

On a more personal note, I have obtained a phone with a display that shows the caller's phone number. If that number shows up as 'out of area' or something I don't recognise, I let my answering machine take the call. Scammers and 'surveyors' seldom dare to leave messages, and nineteen times out of twenty the caller hangs up before the welcome message has even finished playing. This approach appears to be reducing the number of scam calls I receive.