

Scamalot - the scambuster's guide

If it's too good to be true - it's probably a scam! Check it out here.

Rule number 1 - Get a spamblocker

On opening my emails after the weekend, I used to get stacks of pleas from dead dictators' widows to help launder millions of dollars, multi-million pound wins on the lottery, not to mention other unmentionable services I can't mention here. However, I am no longer bothered by this junk. Installing a spam filter reduces stress and saves a lot of time. If possible, go for a web-based one so there is no software to install.

How do these scams reach me?

In this technological age, most scams are sent by email because it's a cheap and easy way for scammers to send their messages out in bulk. You can usually spot scams by the bad spelling or grammar in the title or text; the 'nonsense' sending address; or the urgent tone of the message. More unscrupulous scammers will hijack your url (ie the bit of your web address after the www) and use it as part of their sending address. This gets through the less rigorous spam checkers. Some scams do still arrive by post, but they are usually of the more specialised kind such as items 6, 7 and 8 below.

Scammers have also been known to post messages on discussion boards; and by Skype chat message! So be very careful as they will try anything to grab your attention.

So what's out there?

The following examples are standard forms, but there are hundreds of variations on these themes designed to take you off your guard. If you think you have been the victim of a scam, forward copies to your local police station and inform your bank, if necessary.

Click the links to find out more.

[1. 419 Advance payment](#)

[2. Lottery wins](#)

[3. Requests for bank details \(phishing\)](#)

[4. Boiler Room \(share dealing\)](#)

[5. Money laundering](#)

[6. Mystery shopping](#)

[7. Generous benefactor](#)

[8. Bogus invoices](#)

[419 advance payment](#)



SCENARIO: You receive a message from somebody you have never heard of asking you for help in transferring a large amount of money from their home nation to yours. This somebody might be the widow or other relative of a dead dictator or other high-ranking government official; a bank manager; or a barrister. Very often they will say that they are terminally ill. In return for transferring their millions they promise you a percentage cut of the funds. Sometimes they will ask you to use their money for charitable purposes. Other times they will tell you they are a Christian.

IF YOU REPLY: they will ask you for a sum of money 'for administration purposes'. If you send the money, more 'problems' will arise which will need more money to solve until you realise you are insolvent and will not be seeing any of the promised millions. They may also pass your email address on to other scammers to contact you with other scams.

In extreme cases, people have been known to take large sums of cash in person to the scammer's home country hoping to meet the scammer to finalise the 'deal'. This often results in the victim being attacked and robbed of their money.

These type of scams are called '419-style' after the statute number in the Nigerian legislation which outlaws these fraudulent activities. For examples of how they work see [scamorama](#), but beware as the site contains strong language in places.

[back to top](#)

[Lottery scams](#)

SCENARIO: You receive a message from a company you may never have heard of congratulating you on winning a multi-million sum in their lottery. There is a 'private' contact email address to reply to. Sometimes they tell you not mention the contents of the email to anybody else 'for security reasons'.

IF YOU REPLY: they will ask you for a sum of money for administration purposes. If you send the money, more 'problems' will arise which will need more money to solve them until you realise you are insolvent and you will not be seeing any of the promised millions. They will also pass your email address on to other scammers to contact you with other scams.

Recent messages have been more plausible as they have used the names of established lottery companies including the UK National Lottery.

REMEMBER: You have not won the lottery unless you have bought a ticket! Lottery companies never contact you - you need to contact them if you have won.

[back to top](#)

[Phishing \(on-line banking\) scams](#)

SCENARIO 1: You receive a message seemingly from your bank asking you to re-confirm the logon details and password from your internet banking account. Sometimes these messages will tell you that your account will be suspended unless you comply.

SCENARIO 2: You receive a message purporting to come from the HMRC (tax office) advising you that you are due for a tax refund, or from a respected organisation or trust awarding you a grant.

SCENARIO 3: You receive a telephone call purporting to come from the Office of Fair Trading (OFT) offering to help you reclaim bank charges if you give them your banking details.

In the first two cases you will be asked to click on a link to advise your banking details.

IF YOU CLICK THE LINK: You will be transferred to a website which looks just like the bank or organisation's real home page, but is in reality a clever facsimile built by the fraudster. On the page you will be asked to type in your banking ID and password. If you do this, the scammers will have your bank login details and be able to hack into your bank account, taking all your money.

In most email programmes if you hover your mouse pointer over the link it will reveal the true address to which you are being forwarded. Do not click the link if the destination address looks suspicious.

Sometimes, instead of giving a website address, the email message gives a telephone number which, when dialled, will take you through an automated menu during which time you are asked to type in your account details. Apparently people are more easily duped by telephone calls than websites!

REMEMBER: Your bank or the HMRC will never send you an email asking for your ID and password, and the OFT will not telephone you. If in doubt, telephone your bank, HMRC, OFT or trust fund (on a genuine telephone number) before replying to any of these messages. Most UK banks now have an email address displayed on their login or home page to which you can send suspicious phishing messages.

The banks have combined together to produce a very helpful and informative website about scams and how to recognise them. Click [this link](#) for further details.

[back to top](#)

[Boiler room \(share dealing\) scams](#)

SCENARIO: You receive an unsolicited email or phone call advising you that a company's shares are grossly undervalued and set to greatly increase in value in the next few days. The shares are usually in an obscure name, and you are strongly encouraged to purchase the shares before it's too late.

IF ENOUGH PEOPLE BUY THE SHARES: Market forces will push the value up thus fulfilling the prophecy. The scammers (who very often own the company themselves) will then sell thousands of shares at a profit causing the value to plummet and you to lose your money. Even if you try to sell your shares, most of them are American 'section S' shares which cannot be traded within 12 months of being purchased (by which time the company has probably gone into liquidation).

REMEMBER: There is absolutely no legitimate reason why any stock trader needs to contact complete strangers urging them to buy obscure shares. If you want to invest in stocks and shares, always use a recommended broker or financial adviser governed by the FSA.

[back to top](#)

[Job opportunity \(1\) - money laundering](#)

SCENARIO: An email arrives offering you a position in an established company. The email contains the website address of the company so that you can check for yourself its authenticity. You will be required to receive payments into your personal bank account and pay them on to the company less commission.

WHAT'S WRONG WITH THAT?: Firstly, this is money laundering, which is a criminal offence! Secondly, like phishing scams, the website is a clever copy of the real company's website. It will show the 'job opportunity' on its homepage and invite you to sign up. If you take the bait, it will ask for your banking details which will then be in the hands of the scammers. By accepting the 'job' you may also be getting involved in moving money for criminal activities such as drug dealing or terrorism.

[back to top](#)

[Job opportunity \(2\) - mystery shopping](#)

SCENARIO: You receive a letter from an organisation who requires you to 'mystery shop' Western Union. Enclosed with the letter is a cheque for a four figure sum. You are asked to bank the cheque and then send a proportion of the amount by Western Union to 'test' their banking system. The remainder of the amount is for you as payment for taking part in the 'test'.

WHAT HAPPENS NEXT?: You send the money by Western Union. You then learn that the cheque you paid into your account has bounced. Game over! You lose!

REMEMBER: Most scammers will nominate [Western Union](#) to receive payment. This is because Western Union is not like a conventional bank as it sends money by taking cash from the sender at nominated shops such as newsagents and pays cash out to the recipient at similar outlets abroad using a password and code system. It is a relatively unsecure system and open to fraud. The vast majority of Western Union transactions are legitimate, and indeed I use it myself to send sums of money to my son working abroad as it is easier and cheaper than using a bank. But if Western Union is mentioned in any financial undertaking, do exercise extreme care before parting with your money.

[Generous benefactor](#)

SCENARIO: You receive a cheque for a four figure sum as a donation to your charity from somebody you have never heard of. This somebody spins a plausible yarn persuading you to send back a proportion of the donation.

WHAT HAPPENS NEXT?: You bank the cheque and send some of the money back to the 'donor' as requested. The 'donor's' cheque then bounces leaving your charity out of pocket.

MORAL: Never return a proportion of a donation by cheque unless you are satisfied as to the integrity of the donor.

[back to top](#)

[Bogus invoices](#)

These can arrive by either email or post.

SCENARIO 1: You receive an official looking invoice asking you for a few hundred pounds for an entry into a trade journal or directory. These documents usually have an overseas contact address.

WHY HAVE I GOT THIS?: They are sent by unscrupulous companies to finance departments in the hope they will be paid because somebody will assume somebody else in the organisation has placed the entry. Be smart and throw it in the bin.

SCENARIO 2: You receive a letter from an 'official agency' advising you that you need a data protection licence because by not having one you are acting illegally. They offer to arrange this with the Information Commissioner for a fee of around £120.

REALITY CHECK: Not all organisations need to register with the Information Commissioner's Office (ICO). Even if they do, it costs no more than £35. See the ICO's [website](#) for further details.

[back to top](#)

For more information, please contact [David Wright](#).