15 frauds and scams to avoid

By Nic Cicutti, MSN Money special correspondent

Many of the frauds now being perpetrated are variants of schemes that have been doing the rounds for years, perhaps centuries. What has changed is the means of creating the scam, of hooking and reeling in hapless punters until their wallets and bank accounts have been cleaned out.
In recent years, the internet has given a tremendous impetus to fraud, offering us the "opportunity" to be ripped off not just by a dodgy dealer down the pub, or through a local newspaper advert, but by anyone and everyone, from Portland, Oregon, to Paris, France.

So what are the scams and how do you avoid them? Here's my list of 15 to look out for:

The major scams

There are several that have gained notoriety:

1. "Gifting pyramids", or Ponzi schemes
Named after the celebrated 1920s fraudster Charles Ponzi, this is where you send money, say £100, to 20 people on a list and put your name at the bottom.
In turn the same amount is sent by them to another 20 people each, who repeat the exercise and so on. In theory, when your number comes up, you should eventually end up with thousands of quid.
In practice by the time it's your turn half the world population needs to have joined in the pyramid scheme for you to get a penny. The scammer is, naturally, at the top of the list.
It's a big con, yet every year tens of thousands of people fall for it.

2. "Magazine investment schemes"
Not fraud as such, these are usually advertised in cheap TV guides and gossip magazines where the advertisers assume readers have a low-level of financial knowledge. Quite simply, these are usually old-fashioned with-profits life insurance policies, made even less efficient by spending your precious cash on free gifts.

3. "Boiler room" scams
Boiler room scams are simply illegal and unregulated share trading operations, almost always operating in a different country. Someone phones you up to ask you to invest £10,000 in companies you've never heard of, and which subsequently turn out either never to have existed, or to be non-tradable.

4. "Wine and paintings"
How about a hogshead of malt whisky? Or a rare painting by a celebrated artist? Worth a fortune when you decide to sell and only £5,000 to you, squire.
Except that the whisky turns out to be low-grade stuff, worth a fraction of the price you paid. And the painting is a print, one of 500 whose real value is £38.50. According to the Department of Trade and Industry, in the last three years some £350 million has been handed over on similar duff "investment" schemes.

5. “You have won a free holiday...”
Every day, one of these things seems to fall through the letterbox. There are two types. One is a scratchcard which always seems to reveal a winning symbol, and the other is an official looking letter with “open immediately” emblazoned on it and a certificate visible through the envelope window taking you through to the final round of a “competition”. Your chances of winning are, conservatively, about 87 billion to 1.

6. “Advance fee fraud”
This was a scam once perpetrated by UK conmen on desperate people who needed to borrow money. Loans at a good rate of interest were available, it was claimed, but you needed to pay an “advance fee” to reserve it. Several hundred, sometimes even thousands of pounds later, the money somehow never materialised.
The availability of easy-to-get cheap credit has put paid to most of these schemes.

Today, the approach is more typically from Nigerian emailers. A Nigerian gentleman must get £15 million out of the country and needs you to lend him your account. Your cut will be 10%. There are administration fees of a few thousand pounds to pay but this is nothing compared to what you stand to gain. Isn’t it?

7. “Phishing”
You receive an email telling you there is something wrong with your bank or credit account. But if you log on to this impressive-looking website with the logo of the bank or your card prominently displayed, and enter all your details, they’ll sort it out for you. Indeed they will, as you’ve just given this fake website all your account information and passwords. You might as well start waving goodbye to all your money.

Credit cards

These deserve a section all on their own.
In the past few years, there has been an explosion of card-related fraud, with more than £400 million being tricked out of unwary cardholders’ accounts last year alone.
Clearly, if you lose your card or it is stolen, you can expect that it will end up in the hands of someone who will use it to go on an extended shopping spree, usually followed up with a £50 cash withdrawal at every supermarket they stop off at.
But it’s more sophisticated than that. The way they get hold of your card or its number can include:

8. Skimming
Your card’s details are copied on a special machine (in, say, the back room of a restaurant while you think they are simply sorting out your bill) and used to make a counterfeit one. You think you are safe because your card is secure in its wallet – until the car rental bill comes in. Followed by a visit from police as the car you “hired” disappears.

9. Card-not-present fraud
Your fraudulently-obtained card details are used to make a purchase through the phone, mail order or Internet. Usually the details are taken from a discarded receipt, from a garage forecourt perhaps, or copied from a card without the owner’s knowledge.

10. Identity theft
This involves stealing a person's details and making a card application in their name. Thereafter, two Jack or Jill Smiths appear to be using the same card. Or a card sent to your address is intercepted and used, with a new signature.
Banks and card issuers were meant to have stamped this out through the use of recorded delivery letters and activation telephone calls, in which you have to give some personal details before the card can be used.
But two years ago, my bank somehow managed not to bother with this palaver – as I discovered when my replacement card was used to buy £1,200 of groceries in East Croydon, not to mention a set of wide-rim alloy racing wheels costing £360. Nice.

11. Shoulder surfing
This is where criminals look over a cash machine user's shoulder to watch them enter their PIN number and then steal the card using distraction techniques or pickpocketing. The simpler alternative is where the legitimate cardholder has written down their PIN and kept it with their card in a purse or wallet that is stolen.

In recent years, crooks have become ever more inventive.

12. The charity scam
Criminals are actively using job websites to recruit people to act as forwarders for stolen goods.
For example, let's say I advertise on a genuine job website for "remote assistants", "re-shipping agents", or "correspondence managers".

I say I need someone to sort and forward charitable donations made by hi-tech firms. Sounds plausible – after all, companies often upgrade their IT kit so it seems sensible for them to donate their old stuff to good causes.
I ask you to log on to a website, which looks similar in almost every details to a reputable site. For every package you send on, I will pay you a fee.
Soon, you start to receive laptops, cameras, mini-CD players and all sorts of other hi-fi equipment that must be sent on to an address in Russia or elsewhere in eastern Europe.
Oh, and by the way, I need your bank account details so that I can pay both your postage expenses and your monthly fee directly into it.
You lose out twice over: they'll take you for the postage and they have your bank details. Meanwhile, you have helped spirit several thousands pounds' worth of stolen goods out of the country.

13. Goods not there scam
The simple way is to advertise something for sale at a ridiculous price. You send over the money and…well you can guess whether you receive anything in return.In recent years, scammers have got clever. Take eBay, the largest and most successful auction website, with millions of registered buyers and sellers in the UK alone.
Theoretically, eBay operates a series of controls that ought to keep out the con merchants:

Users are actively encouraged to post pictures of the item they want to sell.
At the end of every transaction, "feedback" is given by the buyer and seller. The more positive feedback, the more reliable the user is deemed to be.
And for the vast majority of transactions this works absolutely fine. But all I need to do is lift a picture of an item, usually a rare collector's piece, from someone's website, and then post it under my name. You bid for it – and it doesn't arrive.

As for "positive feedback" what's to stop me from making a few small purchases of a couple of pounds each, thus gaining precious feedback? I then advertise 20 flat screen 32" televisions at a never-to-be-repeated price of £300 each. Bingo.
Which is one reason, quite apart from complaining to eBay and other websites used to sell items, there is now a growing "vigilante" culture, whereby people are taking their own action against perceived fraudsters.
For example, many clubs keep an eye on bulletin boards and send spam and other insulting email to alleged fraudsters.

14. Nigeria Mark 2
Another way of being ripped off is where someone buys an item off you for £1,000, then tells you they want to pay via a £5,000 cheque. You are invited to send back the change, perhaps by Western Union wire transfer, while keeping £150 for your trouble.
You are clever, so you wait for the cheque to clear first then send them their change. After all, it only takes three to five days, doesn't it?
Wrong. If it's a foreign cheque, it will NOMINALLY be added to your account after five days. But the real clearing takes place only when the cheque's issuing bank, perhaps thousands of miles away, finally does the deed.
At which point you discover that the account over in the US, in Italy or wherever, was fraudulent. And your account suddenly loses the money. Meanwhile you have also shipped the item to a dummy address. Nice one.

15. Fake escrow websites
Of course, you are too clever for any of this. If you are buying, you will hand the money only over to a genuine third party, in return for a small fee, and release it once the item is in the post.
Or if you are selling, the item gets shipped only when the third party says the money is with them. This is known as an "escrow account".
As it happens, at the latest count there are more than 160 known fraudulent escrow websites currently operating throughout the world, with more being added every month.
For reputable escrow accounts, as recommended by eBay but usable for other transactions, click on the following websites:

Escrow.com
TradeSecure
iloxx SafeTrade
Escrow Europa

Finally

Let's say that you have navigated your way round the fraudsters lying in wait for you. You buy the item from a proper reputable website, get it home and are unhappy with it. What next? As it happens, I have written a great article on just this subject:

For extra information on fraud, here are some more sites to visit:
National Hi-Tech Crime Unit at www.nhtcu.org
E-crime Congress 2004 at www.e-crimecongress.org
Cheque and Plastic Crime Unit at www.crimereduction.gov.uk
Computer Misuse Act 1990 on the www.hmso.gov.uk site
Metropolitan Police at www.met.police.uk
Financial Services Authority at www.fsa.gov.uk - the site offers links to fraud information websites

Source:
http://money.msn.co.uk/MyMoney/Insight/MoneySpinner/ThisWeek/scamstoavoid/default.asp