

Title:

Fraud. Beware Of The Fraudsters

Word Count:

983

Summary:

According to Which, the consumer watchdog, about 5 million of us have been targeted by fraudsters and have lost money as a result. Fraudsters are clearly finding rich pickings!

So what are the most widespread scams and how do you steer clear of them? Here are six scams to be aware of.

You've won a lottery prize

Here you receive a letter, or e-mail telling you that you've won a big prize on some lottery you've never heard of. All you have to do is pay an administra...

Keywords:

fraud,identity,theft,phishing

Article Body:

According to Which, the consumer watchdog, about 5 million of us have been targeted by fraudsters and have lost money as a result. Fraudsters are clearly finding rich pickings!

So what are the most widespread scams and how do you steer clear of them? Here are six scams to be aware of.

You've won a lottery prize

Here you receive a letter, or e-mail telling you that you've won a big prize on some lottery you've never heard of. All you have to do is pay an administration fee to claim your prize. The alternative approach is to get you to call a premium phone number to claim.

Guess what - there's no big win and there never was! This scam catches out tens of thousands of people every week.

The "My money is frozen in an overseas account" scam.

It normally starts with an e mail giving a long and involved sob story about someone or some business, which has a very large amount of money tied up in an account and, through the most unfortunate of circumstances, they cannot get the money out. To do so, they need a UK bank account to have the money paid into. Of course, if you help them they will give you a big slice of the money. And the money is always held in a some obscure country, often in Africa.

Another really common fraud. It starts with an e-mail giving a long sob story about someone or some business, which has a large amount of money, often \$ millions, tied up in a overseas bank account. Through the most unfortunate circumstances, the money is frozen and they can't withdraw the money. To do so, they must have a UK bank account to pay the money into. Naturally, if you help them, they'll give you a good slice of the money and you'll be rich!

Invariably the money is always held in a some obscure country, often in Africa. Then, once you've taken the bait, they come up with stage two of the scam. They say that for the money to be transferred to your account, you need to send a payment, often thousands, to cover the administration or legal costs of facilitating the money transfer. The actual details always change, but the bones of the story remain remarkably consistent.

Will the payment arrive? Will you ever get your money back? Of course not! In fact, after you've made a payment, they'll ask for more! The up-front money has to be increased and, unless the extra is sent, the money you've already sent will be lost. It puts you in a classic catch 22 situation. But not really - either way, you'll never see any of your money again!

Millions receive these e-mails every month, so if you get one, delete it.

#### Boiler Room scams

This is a hard-selling technique often targeting middle aged professional people with some but limited investment experience. The fraudsters often trace their targets by searching for small shareholders in the share registers of UK quoted companies.

They then contact their victims by phone or e-mail to persuade them to buy shares in obscure companies on the promise of great returns - all turn out to be worthless. Sometimes they even try to sell shares in companies that don't even exist. Similar versions of the same basic scam involve currency investment, futures or stock options.

If you receive an approach from an organisation trying to sell you investments,

ask for their Financial Services Authority (FSA) registration number. Under the UK's regulations everyone promoting investments must be regulated by the FSA. If they won't or can't supply the number, put the phone down. If they do give you a registration number, don't agree to anything until you've phoned the FSA's help line. There you can check out that the firm is indeed genuine. (call 0845 606 1234). Remember, never commit yourself until you are absolutely sure that the company is reputable. 9 times out of 10 it won't be - you have been warned!

## Credit Card Fraud

The introduction of PIN numbers has greatly reduced credit card fraud. But purchases through the Internet use the "card holder not present" system, not PIN numbers.

This means that if a fraudster can get hold of your credit card details he'll happily use it to buy on the Internet. Then he fades into the mist with the spoils, often to sell them for cash.

To reduce your chances of being caught by credit card fraud, you should sign up to "Verified by Visa" or "Mastercard Secure Code". You'll find further advice about credit card fraud on [www.getsafeonline.org](http://www.getsafeonline.org) and [www.cardwatch.org.uk](http://www.cardwatch.org.uk).

## Phishing

Fraudsters are also highly active on the Internet persuading bank account holders to disclose their banking details, security codes and PIN numbers.

The fraud kicks off with a bogus e-mail apparently from your Bank. The e-mail always explains that for security reasons, it needs you to confirm your account details. Often it says that unless you complete the security confirmation, your account will be frozen. But security is the least of their concerns - once the fraudsters have your bank details, they'll simply empty your account!

You should be aware that Banks never ask you to send them confidential security details by e-mail or by any other method. If the Bank does need to confirm some confidential information, they'll usually ask you to visit a Branch.

## Identity Theft

Every four minutes an identity theft takes place in the UK.

If fraudsters can get your personal details, they can apply for credit and open bank accounts in your name. This inexorably leaves a trail of criminal activity

and debt - all conducted in your name.

All the fraudster needs is a utility bill in your name and a credit card or bank statement. So watch out for unauthorised bin men! Better still, shred any personal letters, bills and documents you need to dispose of.