

get

**SCAM
WISE**

They're just
out to get your
money.

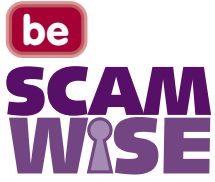
**Don't fall
for it!**

**Advice from Trading
Standards about
Internet Scams**



**SCAM
WISE**
Southwest

**A campaign by
Trading Standards in
South West England
to help stop people
being conned by
rogue traders.**



When you look at your e-mails

The internet has provided scammers with yet another method of contacting people in order to part them from their money and there are many more seemingly fool proof offers for you to “get rich quick”.

Some of the scams used are new, but many of them are old favourites given a new twist for the internet.

“Phishing”

You receive an e-mail from “your bank” or another financial institution, asking you to confirm your account details either by a return e-mail or by directing you to an official looking website for you to enter your details. If you did enter details this would be used by the scammers to drain money from your account.

This e-mail is sent out to hundreds of people in the hope that one will think it is their real bank and bite.

Real banks do not contact people in this way.

If you receive a communication purportedly from “your bank” asking for security details, report the matter to your bank immediately.

In a recent variation on this, some e-Bay customers have been contacted with similar messages supposedly from e-Bay. e-Bay has confirmed that they do not send such e-mails.

Delete all such emails and do not open any attachments



Foreign money laundering

These come as e-mails, faxes or letters, usually from China, Nigeria or other African countries, with requests that you give your bank details so that the writer can 'transfer' money into this country through your account. In return you are offered a percentage of the millions which will be passing your way. The money is often linked to a change in government, a coup or the death of a long-lost relative.

These scams are well-known as international fraud and are investigated by the police.

A website has been set up where details of these scams can be logged – you can find it at

www.nafn.gov.uk

You run the risk of losing all the money in your bank account if you decide to take up this offer.

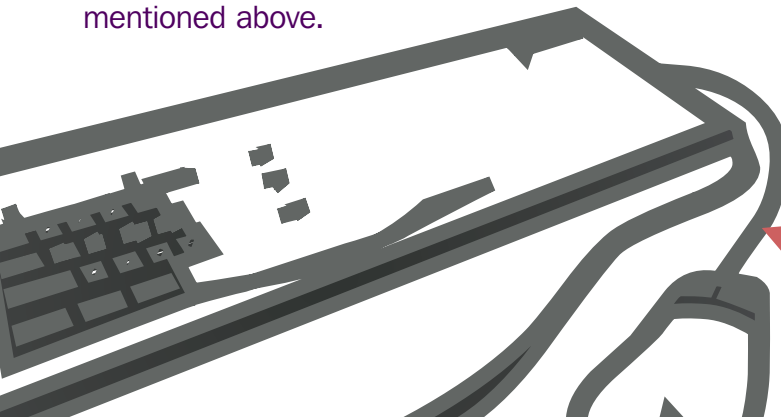
Someone with your surname has died abroad leaving a large estate

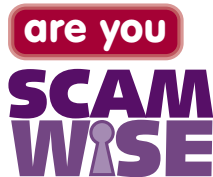
You receive an unsolicited e-mail from abroad. This claims that someone with the same surname as you has died and as they have no other living relatives you are entitled to their large estate simply because you have the same surname. If you do get in touch to try to claim this money, you will be strung along for cash and bank account details in much the same way as if you had responded to the overseas money laundering scam mentioned above.

be
SCAM
WISE
Trading
Standards
say

“Delete junk e-mails”

...and save yourself £££s





About Overseas and other Lottery e-mail Scams?

The Office of Fair Trading (OFT) is urging people not to respond to requests asking them to send money to claim 'winnings' from overseas lottery programmes.

The scam starts when people respond to e-mails telling them they are being entered in a national lottery or some other prize draw, often from Canada, Australia or Spain. They then receive a phone call congratulating them on winning the 'big prize'. However, before they can claim the prize, victims are told they must send money to pay for taxes and processing fees. Often these calls are repeated and further sums are requested.

UK Consumers have lost thousands of pounds through such schemes. The prize doesn't exist, and they never receive any winnings in return for their cash.

These scams usually ask for personal details - full name, date of birth, next of kin, bank account - and once you have given these they will ask for a substantial amount to "claim" your prize, to "register" and to pay "taxes". **DON'T REPLY!**

If you have lost money and become a victim of an overseas scam, the oft would like to hear from you. Contact them by calling

0845 722 4499

Or you can report the matter to Consumer Direct.

Trading Standards say you run the risk of losing the money if you reply to requests and offers like this. The fraudsters will ask for more and more money.

Phone Consumer Direct for help and advice on 08454 04 05 06

Chain Emails

These e-mails are just a modern version of chain letters. You receive an e-mail at your home address telling you of a miraculous way that you can earn vast sums of money. Delete the e-mail from your inbox.

Miracle Cures

You receive an unsolicited e-mail claiming to be able to cure a previously incurable disease or ailment. Trading Standards advise that if a medical claim sounds too good to be true it probably is. Always consult a health care professional before parting with any money for treatments.

Trading Standards advise you NOT to open attachments to e-mails from an unknown source. Delete the e-mails straight away.

Random communications from unknown sources

However interesting these may seem, do not be tempted to open e-mails or attachments from unknown sources. Apart from the risk of viruses, you could find your e-mail box bombarded with further spam e-mails from hundreds of other rogue e-mailers.

Never divulge your e-mail address, personal details and passwords to unknown sources.



About premium rate diallers

You find a large premium rate call or series of calls on your phone bill which you do not recall making. These seem to coincide with times that you were on the internet. If this has happened to you, you may have been the victim of the premium rate dialler scam.

Premium rate diallers are programmes on websites that change your internet dial up number to an 09 premium rate line. The website is supposed to clearly inform you in advance that this is how you will be charged for accessing the site. However certain rogue traders have been installing the diallers on sites where there is no warning. As a result of this people are unwittingly being charged at a premium rate for their entire internet access until the point at which they notice and change the number back - these charges could amount to hundreds of pounds.

One simple way to avoid this scam is to block your internet phoneline from being able to make premium rate calls, contact your phone company about how to do this. If you are a broadband user make sure that the old modem card in the computer is not still connected to your phone socket.

Trading Standards recommend you to complain to ICSTIS, the regulator of 09 phone lines if you have become a victim of this scam.

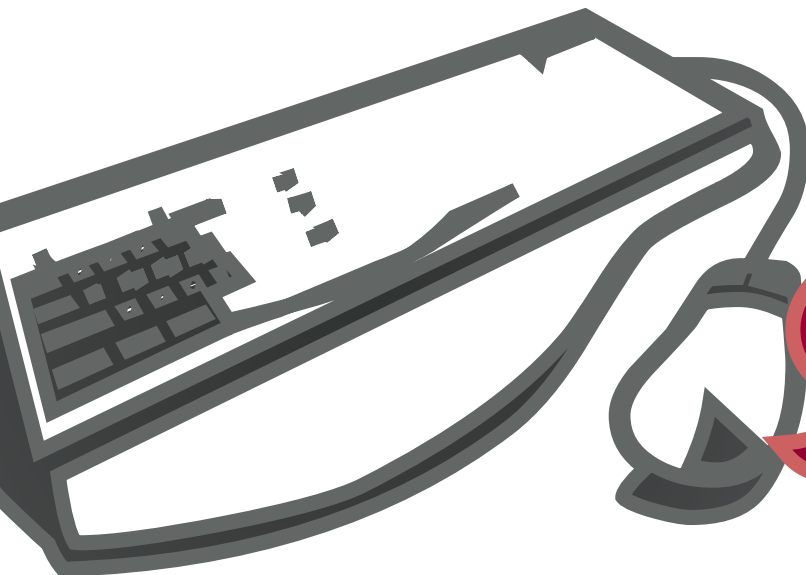
Contact ICSTIS and also check the status of premium rate numbers by calling them on

0800 500 212
or
www.icstis.org.uk



How to avoid Internet and E-mail scams

- Set up your e-mail account so that all ‘spam’ (e-mails from unknown senders) is delivered to your rubbish or ‘trash’ folder.
- Think carefully before opening any e-mails received from people who you do not know - especially if they have an attachment, as these may contain viruses.
- If you receive an e-mail you consider to be a scam then our best advice is to delete without opening it.
- If you receive a communication purportedly from your bank asking for security details then you should immediately report the matter to your bank.
- Install firewalls and anti-virus software on your computer for security.



be
SCAM
WISE
Trading
Standards
say

**“Delete junk
e-mails”**

**...and save
yourself £££s**

stay
SCAM
WISE
about
Internet
scams

If you receive any e-mails like those we have described, simply delete them.

You can help reduce the amount of junk e-mails which you receive by registering with the E-mail Preference Service (EPS).

You can do this by by contacting them at

www.e-mps.org

This will allow you to register a request to members of The Direct Marketing Association not to email you.

**To contact Trading Standards and Consumer Direct
telephone 08454 04 05 06
or log onto www.consumerdirect.gov.uk**



funded by government

Consumer Direct is delivered in partnership with the Office of Fair Trading and local authority Trading Standards across the South West of England.

