HOW TO RECOGNISE SCAMS

Gill Bridle, gives advice about dealing with scams.

Secretary At Work: November 2005 *(reviewed February 2012)*

February 2005 was Scam Awareness month when the Office of Fair Trading with the Department of Trade and Industry worked hard to launch a three-year campaign to combat mass marketing scams.

They issued many tips from 'how to recognise scams' to 'how to protect yourself from scams'. Here is a selection of helpful ideas.

How to recognise Scams

Scam artists

- Are up-to-date and well-organised. They use well-crafted and researched scripts along with professional marketing materials and mailings.
- Are after your money, eg they want you to pay an administrative fee in order to claim a prize or call a premium rate telephone number.
- Have a believable answer to every question. Take time to reflect on what you have been told or read.
- Try to rush your decision. Again take time to consider.
- Steal your trust. They will pretend to be officials from the government, police, bank or a genuine company.
- Steal your personal information. They will demand your bank or credit card details.
- Target everyone. No one is immune.

How to protect from scams

- Check out the company via Internet or a local Trading Standards Dept.
- Do not give bank account or credit card details to someone you do not know.
- If it's a genuine offer there will always be tomorrow.
- There is a scam for everyone.
- New ones are invented every day.
- If you have been taken in, don't be ashamed. It is professional and manipulative conmen that have broken the law. Report it and become a scambuster.
- Trust your instincts – if it sounds too good to be true, it probably is.

Copies of the OFT leaflet 'Scheming Crafty Aggressive Malicious – Don't let them con you' can be obtained by ringing the publication order line: 0800 389 3158.

SCAMS - HOW TO RECOGNISE THEM (PART 2)

Secretary At Work : February 2006 *(reviewed February 2012)*

Most of us are well aware of the potential for scams arriving in the post bag. In addition to these the focus this month is on the internet with especially spam or pop-up messages. This is where internet fraudsters try to lure personal and financial information from their victims and is called 'phishing'.

The Office of Fair Trading is running another campaign throughout February to 'stamp out scams'. This echoes a similar emphasis during February 2005, which is covered on the previous page. This highlighted the various ways people are caught by the clever con merchant and gave tips for clues to identify the 'too good to be true' offers. The current campaign also includes the more subtle ways in which the internet is used to gather personal data.

How does it work?

You will receive an email with similar wording to the following:

> 'We suspect an unauthorised transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity.'
>
> 'During our regular verification of accounts, we could not verify your information. Please click here to update and verify you information.'

The emails or pop-ups claim to be from a business or organisation that you may deal with. The message will always ask you to confirm or verify or update with a direct link to a website which really looks genuine. Sometimes there is also a threat if you do not respond. The bogus site intends to steal your identity and run up bills or commit crimes in your name.

Remember – genuine organisations will never send you emails asking you to update, confirm or validate personal details.

This new breed of phishing email also asks for your online bank details. This can be disguised with giving valuable information on the change to the 'chip and pin' for example but at the end of the email there appears to be a link with on-line banking.

This looks exactly like the bank's web site but it is not. If you enter your login details then you have just given someone else access to your bank account. Never login to your online banking from a link that has been sent to you; always **type** the address of your online bank.

Tips to avoid getting hooked:

- Don't reply to emails or pop-up messages that ask for personal or financial information, and don't click on links in the message
- Don't cut and paste a link from the message into your web browser – phishers can make links look like they go to one place, but they actually send you to a different site
- Use anti-virus software and a firewall, and keep them up to date.
- Don't send personal or financial information – email is not a secure way to send information
- If you are concerned about your account, contact the organisation using a phone number you know to be genuine, or open a new internet browser window and type in the company's correct web address yourself
- Check credit card and bank statements as you receive them and look for unauthorised charges
- As always be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them
- If in doubt ask for advice – call Consumer Direct on 08454 040506