



IMPORTANT INFORMATION for 11th October 2007

EMAIL NEWS

The Harvey Investment Company who were sending job offers to handle cheques through your personal account appear to have changed their name to Draper Investment Company with a new email offering the same kind of part time employment. The new website is owned by a William Shelby in the USA from a server in Germany. The link from the website asks for personal details and details of your bank account. The people behind this scam appear very determined and it must pay them to continue with this.

HM Customs and revenue have the following information on their website: It has come to our attention that **there is a very convincing tax scam** circulating via email. If you receive an email which appears to come from Her Majesty's Revenue and Customs (HMRC) inviting you to apply for a tax rebate, **please ensure you do not fall prey to this scam.**

The email appears to come from admin@HMRC but you cannot reply to this address. The subject line in the example we have seen says "HMRC notification – Tax Refund". Unlike many email scams, the English is generally very good, and many of the embedded hyperlinks work. Clicking on various links takes you to other pages, some of which are genuine HMRC site pages.

The link in the email takes you to a page which asks for credit card details. **DO NOT PROVIDE THESE.** Give-away signs are that the scam asks for your "zip code" (an American expression) and for your "birthday" (the proper request would be for your "date of birth"). Also, hovering your mouse over the link will show it is not a link to the genuine HRMC site.

If you are in any doubt, please telephone your tax office first. If you are really due a tax rebate, the revenue office will normally issue a warrant (cheque) mailed to your home address. They DO NOT ask for your credit card details.

BOGUS CALLERS

Possible bogus Police officers in SOUTH NORWOOD this week. Two white males called at an address and showed an ID card claiming that they were police investigating a missing dog. Neither attempted to enter the premises. They were described as one aged about 20 years, 5'06" tall, medium build and unshaven. He was wearing a grey hooded top with the hood up and blue jeans. The second male described as approx 18 years old with short dark hair and wearing a green hooded top.

BURGLARY HOT SPOT

In the west PURLEY area there has been a major increase in burglaries recently with cash, jewellery, credit cards and small electrical items being taken. They appear to be evenly split between daytime break-ins and night time burglaries

BOGUS CHARITY COLLECTORS

The following usefull information is on the ClothesAid website:

Cheating on charities

So-called 'bogus collectors' prey on the good will of the public and take donated clothing to make a profit for themselves. Typically, the householder will receive a leaflet through the door appealing for donations of unwanted clothing to be distributed to poor families in Eastern Europe or the Third World. Householders are asked to leave the goods in plastic bags by their front door. These are later collected anonymously by unmarked vehicles.

How can I tell if a collector is genuine?

The donation bag should state:

- The charity's name and registered charity number
- The authorised collection agent's name, address and telephone number
- A financial statement indicating what proceeds the charity will receive
- Legitimate collectors should carry identification
- Contact the Charity Commission help line 0870 333 0123
- Contact your Local Authority's Licensing Department to see if the collector has been granted a license to collect in your area
- Check the organisation's or charity's website
- The law requires bona fide charity collectors to carry identification.
- Contact your local trading standards to check on suspicious companies
- You can also check the legitimacy of a company by visiting Companies House website which is www.companieshouse.gov.uk. Bear in mind that status as an active company does not necessarily ensure that its agents are trustworthy

Clothes Aid's own white collection vans are all marked with the Clothes Aid logo and often that of the charity for whom we are collecting. All our collectors wear our smart new uniform and carry Clothes Aid identification.

What should I do if I notice something suspicious

If you are at home, notice who is collecting your bag. Our collectors always carry identification, wear a distinct uniform, and drive vans marked with the Clothes Aid logo and usually a partner charity logo.



Call your Local Police or ring the Clothes Aid help line 0870 607 4600. Any information you give is helpful, including

- The address from where the donation was taken
- The registration number of the vehicle
- A brief description of the suspect

Putting an end to theft

Thanks to the vigilance of members of the public, we have already caught and successfully prosecuted some of these 'bogus collectors'. Clothes Aid is working closely with the Police and Trading Standards to put a stop to this theft once and for all and will always press for the most severe penalties. Please continue to support our partner charities in this way.

It is very important that bag theft does not deter the public from continuing to donate clothing to charities.

Don't let thieves steal your charitable spirit. The proceeds raised through your donations are an important source of charity support.

National Identity Fraud Prevention Week 08.10.07

The UK's third National Identity Fraud Prevention Week began on Monday.

As new research reveals that 79% of us are still being careless with our personal details, an unprecedented group of public and private sector partners have come together to support the UK's largest identity fraud awareness drive. The campaign aims to educate consumers and

businesses as to the dangers of identity fraud, and the preventative steps that could, and should be taken.

Research conducted for last year's campaign showed that 97% of households regularly placed sensitive materials in their waste and recycling bins. The 18% decrease this year shows the impact that campaigns such as this are having in educating consumers about the dangers of identity fraud, and the preventative steps that could and should be taken. The National Identity Fraud Prevention Week 2007 aims to continue this positive trend.

The National Identity Fraud Prevention Week team has once again produced its 'Protecting Your Identity' guide, which is free to members of the public. In addition, an online identity theft risk assessment is available on the official campaign website www.stop-idfraud.co.uk.

For this and more information on how to protect yourself, and how to cope if you are a victim of identity fraud, visit www.stop-idfraud.co.uk, or call freephone **0800 1810 1810** to get a copy of the guide.

Steps you can take to protect yourself from identity fraud include:

- Keep your personal and confidential documents secure.
- Always shred, using a cross cut shredder, before disposing of documentation – bank and credit card statements, utility bills, receipts, direct mail containing any personal information, mortgage applications etc.
- Regularly check your bank and credit card accounts for unusual transactions
- Regularly obtain a copy of your credit report from credit reference agencies Callcredit, Equifax or Experian, and monitor it for discrepancies.
- When you move home, redirect your mail from your old address to your new address for at least a year. You can now apply online 24/7, visit: www.royalmail.com/redirection for more information.
- Going away? If you're planning to be away from home, you'll want to make sure you don't leave any obvious clues, like a pile of mail on your doormat, contact Royal Mail about their 'Keepsafe' service which will hold your mail for up to two months, and deliver it on your return. For more information visit www.royalmail.com.
- Regularly check your bank and credit card accounts for unusual transactions
- Never give out any personal information to unidentified individuals or organisations who contact you by phone, email or face-to-face.
- Visit www.met.police.uk/fraudalert/ for information on different types of fraud.
- Never respond to emails asking for personal or financial information. Be especially careful when sending personal information over the Internet.
- If you receive an email that warns, with little or no notice, that an account will be shut down unless you reconfirm billing or security information, you should not reply or click on the link in the email. Instead, contact the institution cited in the email using a telephone number or web site address you know to be genuine.
- Use up-to-date anti-virus software and a personal firewall and, if your computer uses the Microsoft Windows operating system, keep it updated from the Microsoft website.
- Be extra careful if using Internet cafes or any PC which is not your own and over which you have no control. If in doubt, a good place to get help and guidance on how to stay safe online is your bank's website. Check regularly for specific information and guidance on protecting your PC and yourself online.
- Avoid emailing personal and financial information. Before submitting financial information through a web site, look for the 'lock' icon on the browser's status bar. It signals that personal information is secure during transmission.
- Never give personal information to people calling from companies you have not dealt with before. Always check the identity of these people by calling them back. Obtain their office number from directory enquiries and then confirm their position with the switchboard before speaking to them.
- If you have been a victim of identity fraud involving the use of plastic cards, online banking or cheques, the matter should be reported direct to the financial institution concerned. They will then be responsible for further investigation and, where appropriate, onward reporting to the police. Other incidents should be reported to the relevant organisation and, dependent on their advice, to your local police station.