PROTECT YOUR MONEY

August 2016

Fraud, or "scams", are a common way for criminals to attempt to steal your money. To help you recognise and tackle fraud, Hertfordshire Constabulary's Crime Reduction and Community Safety Department produces this regular update, informing you of common and emerging frauds that are affecting people both nationally and locally, together with tips to help you stay safe and protect your money.

Previous editions of this update can be found at: www.herts.police.uk/ProtectYourMoney

Never Allow Someone To Use Your Bank Account For Their Money – Money Laundering is a Crime

People young and old are being recruited, often unwittingly, to transfer illegally obtained money using their own bank accounts. Criminals use many tactics, including the examples below:

There has been an increase in victims aged over 45 being duped via online dating websites into giving their personal and banking information to a fraudster on the pretence that the fraudster cannot access their own bank account and needs an account to deposit funds they are owed by another business. The fraudster then deposits money into the victim's account, asking them to move the funds to a third party business account.

Also, criminals are recruiting students by advertising fake jobs via newspapers or the internet, often offering opportunities to make money quickly. The student is told to accept money into their own bank account and then withdraw the money or transfer it to a specified account. They are paid a small percentage to do this.

The money has often been stolen from elderly and vulnerable people – sometimes their life savings.

Money Laundering is a CRIMINAL OFFENCE and can lead to prosecution and a custodial sentence. It could also lead to you being unable to obtain credit in the UK and prevented from holding a bank account.

Beware Offers Of Mobile Phone Upgrades

Fraudsters are cold calling members of the public and offering non-existent mobile phone upgrades for really low monthly contracts. After convincing victims to make a purchase, the fraudsters ask for personal and financial details. Armed with this information they then contact the genuine phone provider and order a new phone using the victim's details. They then intercept the delivery or have it delivered to a different address.

Protect Your Money

- Be sceptical and never give your personal information to someone who has unexpectedly called you.
- Independently obtain the genuine number of the business and verify the legitimacy of the caller.
- If an offer seems too good to be true it probably is.

Computer Software Service Fraud: one of our most commonly reported fraud types

In the last year, Action Fraud has received over 30,000 reports and almost £10m in reported losses to this fraud type so please be alert that fraudsters may phone you purporting to be from your internet provider, or a well-known organisation such as Microsoft or Norton Anti-Virus. They tell you there is a problem with either your computer or your internet connection. In some cases, the caller talks you through a process to "fix" the problem, which may involve you unknowingly uploading harmful software or giving them access to your online banking. In other cases, payment is requested for protective software to be installed.

Remember: Computer companies or internet providers will not phone you to tell you there is a problem. Calls of this type are likely to be a scam. If a problem arises with your connection or device, you should call them.

We've also received reports of residents receiving messages on their computer screen alerting them that their computer has been hacked and giving a telephone number to call. This is another form of this fraud.

Do You Sell Items Online?

People selling items on online platforms are falling victim to advance fee fraud. The fraudster, posing as a buyer, sends an email to the seller (victim), agreeing to the full asking price of the item. They state that they are unable to collect the item themselves and will arrange for a courier to pick it up instead.

The fraudster then sends a fake payment confirmation from an email address purporting to be a payment platform. In the following email exchange, the seller/victim is requested to pay the courier fee. Once the payment is made, contact is broken, the item is not picked up and the money paid for the 'courier' is gone.

Protect Your Money

- Be wary of buyers wishing to purchase items at the full asking price without viewing them.
- Always check the validity of a payment receipt confirmation.
- Avoid paying any advance fee if you are a seller. If you choose to use a courier, arrange your own.

Hertfordshire residents receiving bogus calls about council tax arrears

Hertfordshire residents have been receiving cold calls from fraudsters claiming to be council officials getting in touch about council tax 'debt'. The residents are being told that they are in arrears with payments and the caller then demands that they disclose their bank/card details.

If someone contacts you claiming you owe council tax, do not give out your bank details or any other personal information.

Protect Your Money

- Take the caller's name, contact number and the organisation they claim to be calling from and tell them you will call them back.
- Ensure the line has cleared, or, if possible, use a different phone such as your mobile to contact your local council using the advertised number on your council tax bill or from the council's webpage.
- A council tax officer will only ask you for your name, address and council tax number.
- The officer will quickly be able to confirm if you owe such a debt, and whether any debt has been passed to an outside agency working on behalf of the council, such as its enforcement agents (bailiffs).

Fraudsters Selling Vitamins

Hertfordshire Trading Standards have alerted us to a particularly nasty scam where elderly people are being targeted by telephone scammers selling overpriced vitamins to help their health conditions. A 94-year-old Hertfordshire man was told that omega 3 capsules would help to prevent cancer; while another resident, who was repeatedly targeted, lost over £20,000 on unwanted vitamins. Trading Standards has now installed call blockers for these victims to stop future phone calls and has helped to obtain a number of refunds.

Increase In Reports of Ransomeware Affecting Businesses

Ransomware is where criminals lock your computer from a remote location – then display a pop-up window informing you that it will not be unlocked until a sum of money is paid. Most ransomware appears to come from malicious email attachments which have been inadvertently opened and clicked on by a member of staff. For more information visit: www.getsafeonline.org/online-safety-and-security/ransomware

Please report frauds to help us build a picture so that we can warn others. For advice, to report a fraud, or if you think you have been a victim of a fraud or a scam, call Action Fraud on 0300 123 2040 or visit www.actionfraud.police.uk.

Produced by Hertfordshire Constabulary's Crime Reduction and Community Safety Department