PROTECT YOUR MONEY

March 2017

Frauds, 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

IDENTITY THEFT – A WIDESPREAD PROBLEM

Many frauds reported to police and other organisations have been enabled by Identity Theft. This happens where fraudsters have gained enough information about you that they can use your details to commit a fraud, for example to apply for a bank account, loan, state benefit or credit card in your name, or to enter into a mobile phone contract in your name. Identity frauds can have a direct impact on your personal finances and can also make it difficult for you to obtain loans, credit cards or a mortgage until the matter is resolved.

The first you know of it may be when you receive bills or debt collectors' letters for things you didn't order. Some victims have even received penalty notices for vehicles hired in their names.

A Hertfordshire resident recently had his identity stolen after post was stolen from his mailbox. Credit cards and other items were ordered in his name at his address. The new credit cards and other deliveries were intercepted by persons posing as couriers, monitoring his mailbox, which was external to his house.

The fraudsters had undertaken other online research to find out more information about the resident and his family, which also allowed them to "hack" into some of his genuine accounts, including shopping accounts; and goods worth thousands of pounds were ordered.

The whole episode was very distressing for the family, not least because they realised the fraudster must have been watching the house for weeks. It also took time and effort to resolve their bills, cards and accounts.

Protect Your Money

•Consider how your post is delivered. If your mailbox is external your house or if your post is left in a communal area, you may be at greater risk of identity fraud resulting from mail theft.

•Don't leave things like bills lying around for others to look at. Also, never throw out any document containing your name, address or financial details without shredding it first.

•Check your statements regularly and carefully; report anything suspicious to your bank or service provider.

•If an expected bank or credit card statement doesn't arrive, tell your bank or credit card company.

•If you move house, ask Royal Mail to redirect your post for at least a year.

•Where possible, minimise the personal information available about yourself online: your pets' names, family names or other information could be used to impersonate you, crack your password or "memorable phrase".

•These credit reference agencies offer a credit checking service to alert you to changes on your credit file that could indicate possible fraudulent activity: Callcredit • Equifax • Experian • ClearScore • Noddle

•If you receive a letter, email or call from what seems to be your bank asking for your security details, never give your full password or account numbers. Never go to your bank's website via an emailed link; instead, type their full address into your browser.

•If you are concerned about the source of a call from your bank (or other organisation), wait five minutes to ensure the line is clear, or call your bank from another phone, using their published number.

Scam Smart Helps To Tackle Investment Fraud

Investment Scams tend to be the most costly fraud type for individual victims, each losing very large sums.

"ScamSmart is a campaign from the Financial Conduct Authority designed to help prevent investment fraud. The ScamSmart website, www.fca.org.uk/scamsmart, gives tips on how to spot the techniques used by fraudsters and hosts the FCA Warning List. The Warning List is a list of firms and individuals that the FCA knows are operating without its authorisation. A web tool helps members of the public search this list, find out more about the risks associated with investments and the steps they can take to avoid investment scams.

Scam Amazon Emails

Action Fraud has received numerous reports from victims who have been sent convincing looking emails claiming to be from Amazon. The spoofed email from "service@amazon.co.uk" mimics an automatic customer email notification and claims you have ordered an expensive item.

The email states that if recipients haven't authorised the transaction they can click on the help centre link to receive a full refund. The link leads to an authentic-looking website, which asks victims to confirm their name, address, and bank card information.

Protect Your Money

•Be cautious about any unexpected contact, particularly something concerning a gain or loss of your money.

•Think twice: Don't click on links in emails, these can take you to phoney websites which look just like the real thing but are designed to capture your details or load harmful software onto your device.

• If you wish to check on your account, you should do so via your browser, not via a link.

Beware Facebook Links And Ads

It has been reported that residents have typed the word "Facebook" into Google and have clicked on the top search result. It has taken them to a webpage containing a message stating that items were being stolen from their computer and to stop this happening, they should call a given phone number within 5 minutes. They did not phone the number but tried to run an anti-virus scan, during which their computer froze. As a result, they turned off their computer and tried again the next day to switch it on. Upon restarting the device, their phone rang and someone claiming to be from Microsoft has asked to access their computer in order to 'fix' it.

This is similar to other Facebook scams, where people have clicked on a link in Facebook with an eye-catching story, such as a claim that a celebrity has died. Upon clicking the link, a pop-up appears claiming that the computer has been infected and to call a telephone number for assistance.

In any such circumstance, please do not call the number, which will connect you to scammers who will try to access your computer, steal your details and/or try to take your money. Instead, close the windows and run an anti-virus scan on your computer. Please report such incidents to Action Fraud on 0300 123 2040. If you need further help, contact a reputable IT expert, don't deal with any "expert" who has contacted you.

Scam Parking Fine Letters

Action fraud has alerted us to high volumes of letters being sent by scammers claiming to be police/parking authorities informing the recipient they have been spotted illegally parking and have to pay a fine. Be cautious and check the legitimacy of any such contact before responding.