FRAUD PREVENTION UPDATE

January 2015

Fraud, or "scams", has become 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.

BEWARE OF "070" PREMIUM RATE NUMBERS

We are raising awareness of some of the methods used by fraudsters to trick victims into calling apparent mobile phone numbers beginning with "070"which transpire to be premium rate numbers. Calls to these numbers from a landline can cost up to 65p/min and may incur an additional call set-up fee of up to 51p. Calls from mobiles can cost up to £1.50/min. Key methods used by fraudsters to trick you to phone them include:

- Fraudster sends a text or leaves a voicemail/missed call on your phone. You unwittingly call them back.
- Fraudster places a job or other advert online along with an "070" number to call for more information.

If anyone approaches you online or otherwise providing an "070" number, be wary and do not call them.

DONATING TO CHARITIES

Do not be put off giving to charities: they do really important work, but be vigilant and take steps to make sure you are safely giving to legitimate charities. The Charity Commission provide advice, including:

- Fundraising materials should feature the charity's name, registered number and a landline contact number. Be wary of those that list only a mobile number. It is a legal requirement for UK charities with an income above £10,000 a year to provide their registration information on their documentation/website.
- You can search and check the charity's name, registration number and financial profile at the Charity Commission's website: www.charitycommission.gov.uk
- Look for the FRSB tick logo indicating the charity is signed up to fundraising regulation, encouraging you to give with confidence. For details and advice about donating safely, visit www.givewithconfidence.org.uk

PROTECT YOUR BUSINESS FROM IMPERSONATION SCAMS

Businesses are being targeted by organised fraudsters in a number of impersonation scams which pose significant threats to businesses that fail to take security measures to protect themselves, say the National Fraud Intelligence Bureau (NFIB). Some cases have resulted in multi-million pound losses.

One such example is Mandate Fraud, where fraudsters impersonate a supplier you have an existing relationship with, and provide alternate bank details with respect to a genuine invoice, which may have been altered. Another example is Retailer Impersonation, where fraudsters posing as genuine retailers or wholesalers place large orders with suppliers who may or may not have an existing relationship with the impersonated company. The goods are ordered on a credit basis and either delivered or redirected to an address accessible to the suspects, or in some cases, collected directly by the fraudsters who then sell it on.

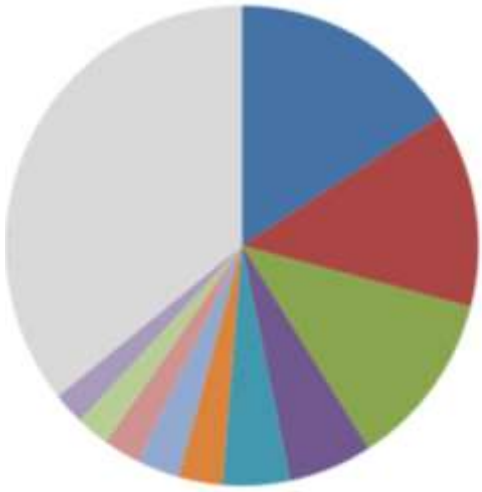
Visit www.ActionFraud.police.uk for advice about protecting your businesses, which includes:

- Always verify new requests for orders, transfers, or changes to financial details by using contact details already on file. Consider using two methods (e.g. email and phone), in case one has been compromised.
- Ensure all staff are aware of these scams and the security protocols in place to identify and prevent them.

Breakdown Of Frauds and Scams Reported In Hertfordshire

Reviewing three months of Fraud Reports by Hertfordshire victims shows that around 100 reports are received each week, about half of which are "Cyber" related (eg. involve online communication or online payments), while the remainder involved contact in-person or via a landline, and a few by post. Around half of all fraud reports indicated that a financial loss had been incurred by the victim, while many others were reported after the intended victim had realised and stopped the fraud before parting with their money.

The below shows the number and proportion of the top ten fraud types reported during this period:



Online shopping/auctions	211	16%
Computer Service Fraud	175	13%
Telephone Scams (Bogus Police/Bank)	158	12%
Cheque, Card and Online Bank Accounts	76	6%
Hacking - Social Media/Email/Personal	61	5%
Loans	40	3%
PPI	39	3%
Retail Fraud	33	2%
Shares/Other Financial Investment	30	2%
Door to Door Sales and Bogus Traders	29	2%
Other	475	36%

Online Shopping: Hertfordshire's highest volume fraud category is "Online Shopping and Auctions" with more than 200 Hertfordshire victims having reported crimes of this nature in the past three months, most involving financial loss to the victim. Although there are many different types of crimes under this category, the majority relate to auction sites, where the victim sent payment but never received the goods. Although this happens in relation to the purchase of a wide range of goods, common purchases relate to mobile phones, cars and vehicle parts. For advice about safe shopping online, visit: www.getsafeonline.org .

Computer Service Fraud: These are phone calls to people at home, where the caller claims to be from a technology company, usually Microsoft. They claim that there is a fault on your computer and they attempt to gain online access to your machine and/or request payment details to fix the problem or supply protective technology (eg anti virus). Most people recognised this as a fraud and ended the call before contacting the police. However some people had lost money. For more information and advice, visit: www.actionfraud.police.uk/news/watch-out-for-microsoft-scam-calls-to-fix-your-computer-jan15

Telephone Scams: These are phone calls to private individuals at home, where the caller claims to be a police officer, fraud investigator or bank employee. They claim that someone has been arrested using your bank card and they attempt to persuade you to either provide them with your PIN number and card, to withdraw your cash from your bank and hand it over for "safekeeping" or to transfer your money online to a "safe" account. Most people recognise the fraud and end the call, but some people reported losses, generally being at high cost. Victims tend to be older people who are at home in the daytime.

Cheque, Plastic Card and Online Bank Accounts: These crimes relate to unauthorised transactions, including withdrawal of funds from accounts, or payments using stolen/cloned cards or cheques. Victims are a mix of businesses and private individuals. For bank security advice, visit www.financialfraudaction.org.uk

For information and advice, or to report a fraud, visit www.actionfraud.police.uk or call 0300 123 2040.