PROTECT YOUR MONEY

June 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

Calls From HMRC – Demanding Payment

We've received a number of reports from residents who have received a phone call from a fraudster claiming to be from the HMRC tax office. The caller claimed the resident owed HMRC an outstanding debt of hundreds or even thousands, of pounds, threatening that they will be arrested unless they settle the debt immediately. They then instructed the victim to purchase iTunes vouchers at a local store to settle the debt. The fraudster then asked them to read out the code on the voucher, enabling the fraudster to redeem the card's value.

The residents genuinely believed what the caller told them, thinking they would be arrested if they didn't settle their debt. Please be alert to this scam. iTunes vouchers allow the download of music and other media from the internet. No government organisation would ask for payment by iTunes vouchers.

Job Fraud

Job fraud occurs when fraudsters purport to be an employer and offer jobs which don't exist. There fake jobs are often advertised in places where legitimate companies offer real jobs. However, the recruitment process will often involve the applicant paying an advance fee, possibly for a background check or for some training. They may also use the applicant's personal details to steal their identity.

Protect Your Money

- Beware paying a prospective employer any advance fees for DBS or other security checks. Don't pay unless you have researched them to ensure they are a legitimate company, possibly by checking with Companies House and undertaking internet/social media searches.
- If the recruitment process involves a telephone interview, the employer should be calling you. Note that some fraudsters might trick you into calling them on premium rate numbers.
- Be suspicious of requests for personal data. Only provide identity/passport/bank details once you have met face to face with your employer and you have the job.
- Be suspicious if an employer/agent contacts you using a non-business email address (such as Gmail or Yahoo), if the job description is poorly written, or if they claim you can "get rich quick". Do not accept job offers where a company requires you to use your own bank account to receive and transfer their money.

Theft Of Mail – To Facilitate Fraud

Fraudsters target homes, particularly in affluent areas, to steal post to identify individuals, such as managers and executives within companies and organisations. Once mail is stolen, research is conducted to identify if the victim is a suitable target. The fraudster uses social engineering to gather information on them and their employer and in some cases then contacts the organisation (purporting to be the victim) to carry out mandate and payment diversion fraud on the company. Fraudsters target banking documentation and personal correspondence. In some cases, fake letterboxes have been placed on homes.

Protect Your Money

- Check where your mail is delivered/deposited for vulnerabilities or tampering. Consider security measures.

Top Ten Tips To Avoid Cyber Crime

If you use the internet, here are our top tips to help you to protect yourself, your money, your identity and your devices:

1. Choose, use and protect your **passwords** carefully, and use a different one for every online account in case one or more get hacked. Use at least 8 digits, a mix of letters and numbers. Ensure your email password is strong and unique, as it could be used to reset other passwords.

2. Look after your **mobile devices**. Don't leave them unattended in public places, and protect them with a PIN or passcode. It's also a good idea back-up your important data.

3. Ensure **internet security software** on computers and similar apps on your mobile devices are updated and switched on. Remember smartphones and tablets get compromised too. Use up to date antivirus and firewalls. If an application provides an update to patch a known threat, then a hacker may be able to gain entry to your device if not updated - So update regularly.

4. Don't assume **Wi-Fi hotspots** in places like cafes or hotels are secure - never use them to do anything confidential. Instead, use 3G, 4G or a VPN (virtual private network). Turn off your Wi-Fi for an hour each week so that a new IP address is allocated. Ensure your home Wi-Fi has a strong password security code.

5. Never reveal **too much personal or financial information** in emails, social networking, dating sites, or in person. You never know who might see it or use it. Do you need to advertise your birth date, phone number, or email? Shred to dispose of any documents containing such information.

6. Always beware that online or on the phone, **people aren't always who they claim to be**. Fake emails and phone calls are a favourite way for fraudsters to approach their victims.

7. **Don't click on links in emails**, posts, tweets of texts – and **don't open attachments** if the source isn't 100% known and trustworthy, or if it seems strange you'd be receiving them. Do not open if unsure of a link. Clicking on a bad link could upload malicious software, which could result in data loss, financial loss or even lock you out of your device. To log in to a website, always go to your bank or other company's homepage by typing their web address into your browser – never via an email link.

8. Never pay for anything by **direct bank transfer** – including goods, services, tickets, travel and holidays – unless it's to someone you know personally who is reputable. Credit cards offer greater protection than most other payment methods.

9. Take your time and **think twice**, because everything may not be as it seems. Remember that if something seems too good to be true, it probably is.

10. For **free expert advice** about all aspects of staying safe online, visit www.getsafeonline.org

PayPal Alert

Fraudsters are using the family and friends personal transaction facility on Paypal to defraud people looking to purchase goods online, such as high value electronics, clothing or footwear. The fraudster asks for payment using the family and friends payment option on PayPal, giving a range of excuses. After payment, the victim loses contact with the seller and the goods are not delivered. By using this service, the victim is unable to raise a dispute as it is not protected by buyer protection, so the victim may be unable to retrieve the funds paid.

Protect Your Money

- When paying by PayPal for goods or services, always pay by commercial transactions (goods or services) to receive buyer protection. Disputes can be raised and funds claimed back if the goods are not delivered.
- Only use the 'family and friends' Paypal payment option to send money to family or trusted friends.
- Avoid paying by bank transfer or money transfer services, as the payment may not be recoverable.