PROTECT YOUR MONEY

December 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.

Further advice and previous editions of this update can be found at: www.herts.police.uk/ProtectYourMoney

Online Relationships

Male fraudsters are setting up profiles of women on dating sites to attract and manipulate vulnerable victims. Posing as women, they use fake images and profiles to target people who are vulnerable and looking for love.

As well as individual fraudsters, it is known that organised criminals based in Africa (often Ghana) and Eastern Europe are involved in Romance Fraud. These networks target UK victims, using profiles to reflect circumstances that potential victims may have, maybe saying they are divorced or bereaved, trying to develop empathy or a special bond. They will take time to develop a relationship; they may develop several potential victims at once.

Once a fraudster is confident they've won your trust, they will tell you about a problem they are experiencing and ask you to help by sending money. Once you send them money, they will invent new reasons to send them more.

UK police figures show that a new romance fraud is reported every three hours, but this is probably the tip of the iceberg, as many victims feel too embarrassed to report their experience. Victims come from all age groups.

Protect Your Money

- Never give money to people you've met online, no matter what emotional story the person uses.
- Pick a reputable dating website and use the site's own messaging service. Fraudsters often try to quickly switch to social media or texting so there's no evidence of them asking you for money
- Don't reveal too many personal details (eg. full name and address) - it may lead to your identity being stolen.

Emails From Well Known Retailers Concerning Your Order

Fraudsters are distributing emails that that look like notifications from well-known online retailers. The emails notify recipients that their recent order has been successfully cancelled or amended. Generally, the order number within the email is a hyperlink. Once recipients click on the link, it leads to a "technical support" message to call a hotline regarding an identified malware infection, license expiration or system problems.

If you call the hotline number, the fraudsters will ask you to give them remote access to your devices to "fix" the problem. They will then harm your device and/or ask for payment or a subscription to "fix" it.

Genuine firms only send order cancellation emails after you have cancelled an order on their website. You can check if you have cancelled an order by using your browser to visit their website and checking your account.

Protect Your Money

- If you have received a notification or cancellation email by a retailer, check the order number matches the order number when you first ordered the product, or check your account for that website.
- If you do click on an order link and a pop-up window appears, you can open your computer's Task Manager (by pressing CTRL+SHIFT+ESC), select the browser under 'Apps', and click 'End Task'. This will let you close the browser or specific tabs even when there is a pop-up or dialog message.

Beware Telephone Calls From Phoney Police Officers or Bank Staff

We are receiving increasing numbers of reports from residents who have been phoned at home by fraudsters claiming to be a police officer or bank official. These fraudsters will give you some basic details such as your full name and address. They may also offer a phone number for you to call to check they are genuine; this number is not genuine and simply redirects you to the fraudster's accomplice.

After trust has been established, the fraudster will tell you that money has been removed from your bank account and staff at your local bank branch may be responsible. You are then asked to help an "investigation" by visiting your bank and withdrawing money to hand to the fraudster or a courier. You may be asked to lie to the bank staff. The fraudster may ask you to withdraw money somewhere else, such as a currency exchange.

Protect Your Money

- Your bank or the police would never call you to ask you to move or withdraw your money.
- Nor would they ever offer to pick up your cash or cards using a courier. Hang up if you get a call like this.
- If unsure, call your bank using their published number or call the police non-emergency number 101.
- If you think you have supplied bank or card details over the phone to someone who has called you who you think is not genuine, contact your bank immediately, inform them of the call and cancel the cards.

Increase In Fraudulent Contacts Regarding PPI Claims

Following the new Financial Conduct Authority (FCA) campaign urging people to make a decision about making a PPI complaint before the deadline on 29th August 2019, we are seeing an increase in fraudsters posing as FCA officials texting and/or cold calling customers and telling them that they are eligible for a PPI claim. The fraudsters say how much PPI you can claim but they ask for an advance fee payment.

Protect Your Money

- Never take up offers of PPI claims on the spot from cold calls and text messages.
- If you wish to use a third party organisation to assist with a PPI claim, you should check to see if they are legitimate. Conduct some online research on them, confirm their business address and landline number, and check the FCA's website for the company's details, as they regulate the financial services industry.

Phoney Trading Standards Officer

Trading Standards have had a report of someone impersonating a Trading Standards Officer, requesting money from a resident to investigate a crime. Genuine TSOs carry official photographic ID issued by the County Council. You can check a Hertfordshire County Council employee is genuine by calling 0300 123 4040.

Unexpected Emails From Police or The Court

We have had several reports from residents who have received emails claiming to be from courts or from the police. The emails have been entitled "You are summoned to court" or other similar wording. These emails encourage you to click on a link or attachment, which will either instigate the downloading of malicious software onto your device or it will lead you to a page that is designed to capture your details. Other emails with similarly fraudulent intentions often claim to be about a speeding penalty or an unpaid debt or tax bill.

Reporting Fraud, Online Scams and Cyber Crimes

If you think a fraud is happening now, for example if someone is at your home and demanding money for what you believe is a fraudulent reason, you should contact police directly. If you think you have been duped into transferring your money or giving someone your bank details, you should contact your bank immediately. If you think you have been a victim of fraud or have been affected by a fraud, report it to Action Fraud by visiting www.actionfraud.police.uk or by calling 0300 123 2040.

Opportunities within Horse Racing appear to be a trend emerging in Investment Fraud. The National Fraud Intelligence Bureau (NFIB) have received complaints where the suspects claimed to use software for placing bets on horse racing on the victims behalf. This has been pitched as an investment opportunity. Once money has been sent to the fraudsters, methods of contact are closed and the victim does not hear from them again.

PROTECTION / PREVENTION ADVICE

 Investment into a racing horse as part of a syndicate may in some instances fall within a collective investment scheme and therefore may be subject to FCA regulation. Consumers are advised to consult the FCA guidance which can be found here; https://www.fca.org.uk/consumers/unregulated-collectiveinvestment-schemes Betting syndicates do not require a licence from the Gambling Commission or British Horseracing Authority therefore caution should be exercised before parting with any money Always check that the details of the organisation or company contacting you (such as website, address and phone number) are correct – the fraudsters may be masquerading as a legitimate organisation Never respond to unsolicited phone calls – if in doubt, hang up Don't be fooled by a professional looking website (or brochure) as the cost of creating a professional website is easily affordable Consider seeking independent legal and/or financial advice before making an investment

The National Fraud Intelligence Bureau (NFIB) has received intelligence that fraudulently obtained funds from multiple timeshare recovery frauds have been transferred to a number of bank accounts, of which the beneficiaries reside in the North West of England.

Fraudsters are cold calling victims of previous fraudulent / mis-sold timeshare schemes and are claiming to be from legal firms or the Spanish authorities. The individuals calling are falsely advising previous victims that they are owed compensation and simply need to pay some fees to obtain this money. The fraudsters are aware of the victim's details and possess knowledge of their previous investment, giving them false credibility.

PROTECTION / PREVENTION ADVICE

 Be aware of fraud recovery scams if you've been a victim of fraud in the past. Challenge/ignore any calls, letters or emails from people you don't know or companies you've never contacted yourself.

 Always check that the details of the organisation or company contacting you (such as website, address and phone number) are correct – the fraudsters may be masquerading as a legitimate organisation. Never respond to unsolicited phone calls – if in doubt, hang up. Consider seeking independent legal and/or financial advice before making any financial investment. If you have been affected by this, or any other scam, report it to Action Fraud by visiting www.actionfraud.police.uk or by calling 0300 123 2040.

Action Fraud has received intelligence suggesting that rather than setting up fraudulent accounts, fraudsters are advertising bogus online sales roles on job vacancy websites in the hope of attracting unsuspecting jobseekers. Once a jobseeker has shown interest, the fraudsters tell them they will be selling goods on the company's behalf; often the goods are cars or machinery but they could be anything. Jobseekers are also instructed that they must use their own personal pre-existing bank accounts and payment methods, as well as their own online marketplace accounts. The fraudsters usually give a vague excuse as to why a business account or login is not available. Jobseekers are then sent photos and information of the products they will be selling (which do not exist) in order to create an attractive advert to entice the primary victim; the buyer of the goods. Once the victim has transferred their money to a bogus escrow provider, no goods are ever received and all contact is severed. This leads to a financial loss for the buyer of the goods as nothing is ever

received. Likewise, the recruited jobseeker receives none of the promised payment for their work as originally stipulated in the bogus advert.

*Escrow – An escrow is a type of agreement where a third party becomes involved in a financial transaction; an escrow provider will hold a sum whilst the transfer of goods or services is facilitated between two other parties. Upon transfer, the escrow provider will then release the funds as appropriate. Genuine escrow providers can be useful, however fraudsters frequently impersonate them for their own financial gain.

Protect Yourself

Buyers

 When making a large purchase such as a new car or machinery, always meet the seller face to face first and ask to see the goods before transferring any money. False adverts often offer goods for sale well below market value to entice potential victims; always be cautious. Exercise caution when sellers state that they are selling on behalf of a friend, colleague or business.

Jobseekers

 Don't assume advertised vacancies have been verified by the website or classified advertisement sites upon which they feature. If you suspect a job vacancy to be fraudulent, be sure to notify the website via their reporting/flag functions. Doing so prevents others from becoming victims of fraud and helps organisations and law enforcement tackle and disrupt fraudulent activity. Although many legitimate job vacancies are internet based sales roles, those which are vague about the business, product type, sales method or sales platform to be used should be approached with caution. It is always good practice to conduct further enquiries about an advertised role. Genuine businesses would never ask you to use your personal bank or online payment accounts to facilitate business transactions, nor would they ask to utilise your personal online marketplace account in order to sell their products. If someone claiming to represent the organisation suggests you do this or asks for your personal details so they can use your account(s) themselves, sever contact.

The National Fraud Intelligence Bureau (NFIB) has identified a number of reports where job seekers are being targeted by fraudsters trying to obtain personal and banking details from them, or requesting money to secure accommodation.

Individuals registering with job seeking websites or searching for jobs on The Student Room website are being contacted by bogus recruitment companies/businesses asking them to complete application and interview forms which request personal details and banking details, as well as copies of identity documents.

In some instances the applicant is invited along for interview, either in person or over the phone, to make the process look as legitimate as possible. This is impacting on students and graduates looking for work both in the UK and overseas. Some job seekers, as well as divulging personal details, have paid money to the fraudsters in order to secure a bogus rental property alongside the job offer.

How to protect yourself:

- Check emails and documents from the recruiter for poor spelling and grammar – this is often a sign that fraudsters are at work.
- If visa fees are mentioned, ask the embassy representing the country where you believe you will be working how to obtain a visa and how much it costs. Check that the answers the potential employer or recruiter gave you are the same – if they're not, it may be a sign of fraud.

- Carry out thorough research to confirm that the organisation offering you the job actually exists. If it does exist, contact the organisation directly using contact details obtained through your own research or their website to confirm the job offer is genuine.

POLICE.UK Crime and policing in England, Wales and Northern Ireland

You've been witness summoned to court

You are herewith summoned to attend to court to give evidence.

It is extremely compulsory that you declaim the subpoena you received very carefully. This will state exactly what the pocess will be if you break down to do what is demanded of you. Sincerely Witness Care Unit agent **Tony Munk.**

Please, view court location and case information

VIEW CASE DETAILS

This email is the part of The Crown Prosecution Service online notification project.

POLICE.UK Crime and policing in England, Wales and Northern Ireland

You are summoned to court

You're hereby summoned to visit to court to give confirmation.

It is extremely binding that you declaim the subpoena you received very attentively. This will state specifically what the procedures will be if you fall through to do what is demanded of you. With regards Witness Care Unit agent **Theresa Keller.**

Please, view court location and details of case

VIEW CASE DETAILS

This email is the part of The Crown Prosecution Service online notification project.

Expecting A Delivery?

Scam "missed delivery" cards are being posted through letterboxes that look like they are from Royal Mail.

Action Fraud have alerted us to 'something for you' cards arriving through letterboxes that look similar to the 'something for you' slips that are posted into homes by Royal Mail if a delivery can't be made. To arrange a redelivery, the scam cards urge recipients to call a 0208 number, which is not registered to Royal Mail.

Recipients should consider whether they are expecting a delivery from the company named on the card, and if in doubt, do not call the number provided, or if you do, don't give out any personal details. You can arrange a redelivery by Royal Mail via their website, www.royalmail.com. Their enquiries number is **03457 740 740.**

Alert For Students – Student Loans Scams

Action Fraud are asking us to alert first-year and returning university students to a scam email that claims to be from The Student Loans Company. Victims are duped into entering personal information that is then being used to steal their identity, enabling the fraudsters to obtain documentation, goods or credit in their name.

The fraudulent email has come to light in the lead up to the new academic year. It claims that Student Loans Company accounts have been suspended due to incomplete student information. It urges the recipient to update their details via a web link which leads to a fake website designed to harvest personal details.

The scam appears to target both new and current university students. However, some individuals who have never applied for student finance have also received the email.

Police advise that you should never click on emailed links or log into any organsiation's website via an emailed link. Instead, you should type the organisation's correct web address into your browser.

Protect Your Pension

If you are contacted out of the blue with offers of 'free pension reviews', 'government initiatives', 'guaranteed rates of return', 'access to cash before age 55', or couriers who will help you complete the forms, then please beware that these are commons signs of a pension scam.

Impressive company literature, smart websites, knowledgeable representatives and professional looking marketing materials are also no guarantee of a firm's authenticity.

The Pensions Advisory Service (TPAS) (www.thepensionsadvisoryservice.org.uk) provides independent and impartial information and guidance about pensions, free of charge, to members of the public. We help with all pension matters covering workplace, personal and stakeholder schemes. We answer general questions, help with specific queries and offer guidance for people with complaints about their private pension scheme.

If you'd like to talk to TPAS about an offer you have received or think you may already be being scammed, please call **0300 123 1047**. TPAS is there to help you with any pension related question.

Do you sell items online and use PayPal?

We have received several reports recently where local residents have lost items or money after they believed they had sold items online to purchasers using PayPal. The two most common scams were:

The buyer sends money via PayPal but asks for item to be sent to a different address, such as their "work address" or a "gift address". The victim receives the payment and sends the item to the new address. The buyer then claims they did not receive the item and requests a refund. Because the seller sent the item to a different address, they are not covered by PayPal's seller protection, so the buyer receives their refund and the seller ends up with neither the items nor the money.

The buyer tells the seller that they will pay by PayPal. The seller then receives an email (that looks like a normal PayPal email) confirming payment has been received. The seller then sends the item. However, the PayPal confirmation email was fraudulent and the payment was never made.

Protect Your Money

- Don't accept an email as proof of payment, always check your account to ensure monies have been received. Log in to your Paypal account via your app or browser, never via an emailed link.
- Please bear in mind when selling items, PayPal's User Agreement includes: "A key eligibility requirement of the Seller Protection Programme is that, for tangible items, the seller must post the item to the address which appears on the transaction details page."
- To view the PayPal User Agreement, visit www.paypal.com/uk and click on "Legal" in the bottom right hand corner of the page.

Our Most Commonly Reported Scam Involving Over 60's

Computer software service fraud is when a resident receives a telephone call from someone claiming to be from Microsoft, BT, Virgin or another well known technology or internet company. The caller says there is a problem with the resident's computer or internet connection and that they can fix it.

In most cases, the victim is cold called, but recently we have seen an increase in contact via a pop-up on the victim's computer prompting them to phone the fraudster, believing the pop-up to be from a genuine source.

The victim is persuaded to grant the fraudster remote access to their computer and provide payment details for the fix. The fraudster then uses a variety of methods to obtain access to the victim's bank account to take large sums of money. The fraudster may also install software which could potentially be malicious. The victim may be contacted again later and told they are due a refund and they are again asked for access to their account. The fraudster will use this opportunity to take even more money.

Protect Your Money

- Remember - Any unexpected contact from a technology company is likely to be a scam. Technology or communications companies would never phone you to tell you there is a problem with your computer or internet connection. They always wait for you to phone them to report a problem.
- Likewise, they would never send a pop-up to your computer with a phone number to call. If you need to contact them, you should source their number from your documentation or from their official website.

Hertfordshire Trading Standards Twitter Account

Our local Trading Standards are keeping people updated about scams via their Twitter account. Follow @HCC_TS for their latest scam advice.