



HERTFORDSHIRE
CONSTABULARY

PROTECT YOUR MONEY

November 2016



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

TEN STEPS TO PROTECT YOUR PENSION

Many people have lost their life savings after falling for a pension scam. If you’re thinking about how to invest your retirement savings, follow The Pensions Regulator’s ten steps to protect your pension:

1. Be wary of cold calls and unsolicited texts or emails: Scammers often claim they’re from Pension Wise or other government-backed bodies. These organisations would never phone or text to offer a pension review.
2. Check everything for yourself: People have fallen for scams that were 'recommended by a friend'. Do your homework, even if you consider yourself financially savvy - false confidence can lead to getting stung.
3. Ensure your adviser is on the Financial Conduct Authority approved register: Pensions scammers may pose as financial advisers. Check to make sure yours is registered on the FCA website.
4. Check the FCA's list of known scams: Visit www.scamsmart.fca.org.uk - are you being sold a known scam?
5. Steer clear of overseas investment deals: common scam types include unregulated investment in a hotel, vineyard or other overseas opportunity, where your money is all in one place - and therefore more at risk.
6. Don't fall for 'guaranteed' returns or professional looking websites or brochures: You can never guarantee returns on investments, and anyone can create a smart website or brochure these days. Question everything.
7. Don't be rushed into a decision: Scammers may pressure you with 'time limited offers' or send a courier to your door to wait while you sign documents. Take your time to make all the checks you need - even if this means turning down an 'amazing' deal.
8. If you're aged 50 or over and have a defined contribution (DC) workplace pension, talk to Pension Wise: Pension Wise is there to help you investigate your retirement options. Visit www.pensionwise.gov.uk for more information (and to check what kind of pension you have).
9. Ask The Pensions Advisory Service for help if you have doubts: You can call them on 0300 123 1047 or visit the their website for free pensions advice and information: www.pensionsadvisoryservice.org.uk
10. Contact your provider and call Action Fraud if you've already signed and think you've been scammed: If you've already signed something you're now unsure about, call Action Fraud on 0300 123 2040 and contact your pension provider immediately. They may be able to stop a transfer that hasn't taken place yet.

LATEST EMAIL SCAMS TO AVOID

Fraudsters are sending out a new wave of scam emails entitled “You’ve been witness summoned to court”, purporting to be from the Crown Prosecution Service (CPS) and claiming you have to appear in court. Another email entitled ‘compensation fund’ is currently in circulation claiming to be from the City of London Police ‘National Fraud Intelligence Bureau’ or ‘Fraud Intelligence Unit’. It has a letter attachment offering financial compensation to fraud victims, stating that for compensation to be arranged, the recipient should reply giving personal information. These emails are both fraudulent and should be deleted. These are the latest email scams in circulation, but many others continue to be reported, including those claiming to be from your bank or a government department . Remember that opening attachments or clicking links contained within emails from unknown sources could result in your device being infected with harmful software (known as malware).

AMAZON PAYMENTS AND ONLINE SHOPPING ADVICE

One of our members recently reported that while searching the internet to buy an iPhone he came across a remarkably low price on Amazon. He went to the Amazon website and found an Amazon Marketplace provider offering the low price. However, it was not possible to order the item on the Amazon website, the seller requested email contact before ordering. After emailing, a reply arrived to say that the product was available and giving assurances that any purchase was backed by Amazon money back and return policy. The email asked for his details and said that an Amazon order would follow outlining the process. An email then arrived which looked like a scanned Amazon page, asking for a bank transfer, despite the email saying that payment would be handled by Amazon payments. It said once payment was received, the order would appear in the buyer's Amazon account. The member recognised this as a scam and contacted Amazon to report it.

Protect Your Money

- When making online purchases, remember never to use direct bank transfers to people you don't know. Fraudsters often concoct stories to convince you to transfer your money to a bank account instead of paying by a safer method – be suspicious of anyone asking you to do this.
- Remember that credit card payments offer greater protection than many other methods. Alternatively, use a secure payment site such as PayPal – but beware phoney PayPal emails.
- Amazon's website has a "Help and Customer Service" section, within which is a "Payment Methods" page with guidance and advice about payment methods.
- Before making any purchases, research unfamiliar retailers online. It is also a good idea to conduct a 'whois' search at <https://who.is/> to check when the site was created, be wary of newly formed domains.
- For more advice about online shopping and auctions, visit www.herts.police.uk/protectyourmoney

BEWARE BINARY OPTIONS

Whilst marketed as investments, Binary Options are essentially bets on whether certain prices within financial markets will rise or fall. You can bet on whether a company's value or commodities such as oil or gold, will go up or down within a given timeframe. There are only two outcomes with this type of investment: cash or nothing. Guess correctly to win, or incorrectly and lose all the money you have invested; hence the term "binary". Fraudsters are using social networking sites and apps to lure potential victims with the promise of guaranteed returns on their investments. However, Binary Options trading is not a regulated financial activity in the UK, so you will not be covered by the Financial Service's Compensation Scheme if things go wrong.

THINK TWICE BEFORE YOU INVEST

Recent figures show that 3,186 investment frauds were reported to Action Fraud in 2015/16, that over 77% of victims reporting investment fraud were men with an average age of 65. Their average loss was over £32,000.

You are usually contacted out of the blue by a professional-sounding broker offering investment opportunities that seem too good to miss. You may be promised free research reports, special discounts and 'secret' stock tips. Fraudsters aim to make their business seem legitimate; they often use technical jargon, impressive job titles and smart websites to appear credible. They will do everything they can to manipulate potential victims and convince you that they are making genuine investments. Unfortunately, once sucked-in by a fraudster, victims often end-up parting with significant amounts of money and this can have devastating effects on both the individual and their families.

Protect your money

- If you're considering any type of investment, remember: if it seems too good to be true, it probably is.
- Visit the Financial Conduct Authority's (FCA) ScamSmart site for advice on making safe investments.

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.