

|  |
| --- |
| **PROTECT YOUR MONEY** |

**Advice from Hertfordshire Police about how to avoid becoming a victim of fraud and scams**

**You receive a phone call from Detective Inspector Morris at Islington Police Station…**

He tells you that they have just arrested two people in a shop in London and one of them was found to have a bank card in your name…

**He is concerned that your bank account may be in danger…**



This is the beginning of a common scam in Hertfordshire and across the UK.

Many Hertfordshire residents have lost large sums of money after they followed instructions given to them by fraudsters posing as either police officers or bank officials.

This booklet aims to alert you to some common scams impacting on local residents and how to avoid them.

As average life-expectancy increases, we have a growing number of older residents within our local population.

While most reported frauds, like other crimes, involve younger people as victims, some frauds or scams are targeted at older people.

Many older residents have accrued savings or receive regular income from pensions, so some criminals target this.



**OUT AND ABOUT**

When making a payment, ensure you use your hand and body as a shield while entering your PIN number. Take care to put your card away afterwards. Purse thefts often occur after thieves have watched someone entering their PIN.

Keep your bag or wallet secure at all times. Beware strangers approaching you and asking questions, particularly in shops and car parks. They may be trying to distract you into looking away from your bag so they can take it.

**ADVANCE FEE FRAUD**

The most common fraud type affecting the over 65 age group is “advance fee” fraud, where fraudsters persuade victims to make up-front payments for goods, services or financial gains that do not then materialise.

**Beware anyone asking for payment in advance…** …such as “administration fees”, “tax”, “transport fees” or “deposits”

Treat with extreme caution anyone who has contacted you to request you send money or make a payment for any reason. If you do not know this person, you cannot be sure they are who they say.

**Scams come in many forms and try to exploit a number of themes:**

* **Danger/urgency:** 
  + Your bank account is in danger
  + Your roof or guttering is damaged
  + A tree in your garden is dangerous
* **Offers of help:**
  + There is a problem with your computer or internet
  + You need some maintenance work on your home
  + Offers of dietary supplements or vitamins
* **Requests for your help**:
  + Please support our charity
  + A friend or family is stranded and needs money
  + Someone needs to borrow money or asks to use your bank account for their money
* **A bogus official**:
  + Your bank emails to ask you to confirm your details
  + You have a parcel awaiting collection
  + You are owed a tax rebate
  + You are contacted by the Home Office or the Police
* **A financial opportunity**:
  + You are owed a PPI refund
  + You have won a lottery or prize draw
  + You have inherited money from a distant relative
  + You are offered a way to enhance your pension
  + You are offered an investment opportunity

**All these tricks have been used to steal money from local people this year!**

**Common Frauds**

**EXAMPLE 1**



**The Phoney Police Caller**

You receive a phone call from the police or your bank.   
They think your bank account may be in danger.

They may ask you to put the phone down and call   
the police for your bank to confirm who they are.

He may even ask you to check your caller display   
(if you have one) so that you can see they are calling from your bank.

You may then be asked to withdraw or move your money. You may be asked to provide your PIN number or send cash or your bank card to them via a courier.

**Beware of this scam which has affected many older residents in Hertfordshire.**

Fraudsters have the technology to imitate another phone number so that your caller display shows a number that is familiar to you, even if they are actually calling from somewhere else.

Also, fraudsters will keep the line open, so when you hang up and then call the police, you unwittingly re-connect to the fraudster, who may then pretend to be the police switchboard. So, always use a different phone or check the line has disconnected by firstly phoning someone you know and would recognise.

**REMEMBER:**

The police or your bank would **NEVER** telephone to ask you to withdraw money or move your money to another account for “safe keeping”, “evidence” or for any other reason.

The police or your bank would **NEVER** ask you for your bank card’s four-digit PIN number. You should never tell anyone this number, it is for you to use at cash machines or shop payment machines only.

**EXAMPLE 2: The Computer Fixer**

You receive an unexpected phone call from someone at your internet or telephone company, such as BT or TalkTalk. They have detected a problem with your computer connection and want to fix it for you. They need to gain remote access to your computer or talk you through a process to fix it or install “anti-virus”.

**This is a common scam in Hertfordshire.**



The changes made to your computer may be harmful, such as programmes that steal your data. In some cases, fraudsters have gained access to the victims’ online bank accounts and have taken their money.

Remember: Firms like BT or Microsoft would not call you to fix a problem; they would wait for you to report a problem to them. Never let an unexpected caller talk you through a process nor should you allow them to access your computer.



**EXAMPLE 3: You Are Owed A Refund**

You receive a telephone call: you are entitled   
to a PPI or tax refund of more than £1,000.

But before your refund cheque can be released,  
you need to pay a “fee”, possibly using a money  
transfer service like “Western Union” or   
“Moneygram”. Alternatively, you may be asked to  
buy iTunes vouchers. These payment methods are favoured by fraudsters.

This is a common scam, tricking you to send money in order to receive some money that will never materialise. Refuse any requests for payment by iTunes vouchers or money transfers, such as “Western Union” or “Moneygram”, as once the money is collected, the collector is untraceable and your money is lost.

Note: Credit card payment generally offers greater protection in terms of fraud.

**EXAMPLE 4: The Rogue Trader**



You receive a caller at your door offering to repair some damage to your roof that he’s seen.

He can carry out the work today, but will need some payment in advance for materials.

He offers to give you a lift to the bank so that you can collect the cash.

Do not deal with doorstep tradespeople. We receive numerous reports where people have later been overcharged or work has been of a poor standard.

If you think gardening work or repairs are needed at your home, seek a second opinion from someone you trust. Contact a reputable trader, and seek a written quote before work commences. You should not be asked for up-front payment.



**For a Trading Standards recommended   
tradesperson, contact Trading Standards  
on 08454 04 0506 or visit**

[**www.trustedtraders.which.co.uk**](http://www.trustedtraders.which.co.uk)

To deter doorstep traders and other unwanted  
callers, it is a good idea to display a “no cold  
callers” sticker in your window and then politely  
turn away any callers that you do not know.

Genuine callers won’t mind returning at an agreed time when you can arrange to have someone you trust with you.

**EXAMPLE 5: Scam Mail**

You may unwittingly be on what criminals cynically call a “suckers list” and end up receiving lots of post from fraudsters posing as lotteries, prize draws, solicitors, clairvoyants or charities. Scammers often use colourful envelopes and language like: “Act Now” or “Guaranteed Winner”, promising cash prizes if you place an order. It is best not to respond to any mail of this kind.

If you think you’re receiving scam mail, Trading Standards can help.

**EXAMPLE 6: Scam Emails**

You receive an email from a well known business or organisation, such as your bank, Amazon, the Tax Office, or a delivery company, asking you for information or to confirm some details or instructing you to click on a link or attachment.

Remember that online, people aren’t always who they claim to be. Fake emails are a common way for fraudsters to approach their victims.

Never click on an attachment or link in an email unless the source is 100% trustworthy, and never go to your online banking via an email link. Always visit websites such as your bank by typing their full web address into your browser.

**OTHER RISKS**

* Making any large financial investment, such as in property, art or shares.
* Booking a holiday or buying a second hand vehicle.
* Meeting new people online: romance fraud often affects older people.

Advice is available at: [**www.actionfraud.police.uk**](http://www.actionfraud.police.uk/)[**www.GetSafeOnline.org**](http://www.getsafeonline.org/)

**TOP TIPS TO PROTECT YOUR MONEY**

* Never let an unknown person into your home
* Don’t deal with doorstep traders
* Beware unexpected calls and emails: fraudsters may pretend to be officials
* Don’t allow yourself to be pressurised by pushy sales techniques. Take   
  your time – why not seek a second opinion from family or friends?
* Never send money to anyone you don’t know personally, and never pay  
  fees to claim lottery winnings, inheritance or tax refunds
* Avoid cash payments, iTunes vouchers or money transfers.
* Credit cards offer more protection than most other payment methods
* Never tell anyone your bank card PIN number
* When entering your PIN in shops and cafes, use your hand as a shield

**IT IS A GOOD IDEA TO JOIN NEIGHBOURHOOD WATCH**

**1 in 3 homes across Hertfordshire have already joined us!**

We send regular updates to our members to inform them about the latest frauds and scams affecting Hertfordshire residents, together with advice about how to spot scams and avoid becoming a victim.

We will also provide you with other useful information from your local policing team, including prevention advice about different types of crime to help you to [www.owl.co.uk/herts](http://www.owl.co.uk/herts)  
keep yourselves, your homes and your property safe.

We will keep you updated by email, or by telephone message if you prefer.

In addition to our Neighbourhood Watch service, we have a new service:

**SENIOR WATCH**

**SENIOR WATCH** provides messages specifically aimed at informing our older residents about frauds, crimes and local issues affecting them. It also includes signposting of local services for older residents.

**SENIOR WATCH** members can either sign up to the service themselves, or can provide details of a trusted person to receive the email messages on their behalf and keep them informed. For more information, contact the Watch Liaison Team on the police non-emergency number, 101 or via [**wlo@herts.police.uk**](mailto:wlo@herts.police.uk) or you can register at [**www.owl.co.uk/**](http://www.owl.co.uk/)**senior**

|  |  |
| --- | --- |
|  | **You’ve worked hard to save your money, so you should spend it as you decide…**  **don’t lose it to fund a criminal’s lifestyle!**  **www.herts.police.uk/CrimePrevention** |