This information hub is designed to provide the reader with current and emerging scams. We hope you will find it of interest.

If you would like to share with us any information on scams, please email us at scamsawareness@agecymru.org.uk

**Scams Awareness Month: Creating a united front against scammers**

A unique initiative is bringing public, private and third sector organisations together to make Wales a hostile place for scammers, criminals who often deliberately target older and vulnerable people.

The Wales Against Scams Partnership (WASP), whose members include Age Cymru, the Older People’s Commissioner for Wales, and trading standards, is using Scams Awareness Month to highlight the nature and impact of scams within communities across Wales.

Scams against older and vulnerable people can take many forms, with criminals targeting individuals via the post, over the telephone and door-to-door. Recent years have also seen a significant increase in scams and fraud perpetrated via the internet.

The cost of these scams is not simply financial: victims often suffer a loss of confidence, self-esteem and peace of mind and in many cases feel a sense of shame, which can lead to a failure to report crimes of this nature – figures show that less than 5% of victims report scams to the authorities. The impact of scams can, quite simply, blight the rest of an individual’s life.

Ian Thomas, CEO of Age Cymru and Chair of WASP, said: “During Scams Awareness Month, it is vital that people gain a greater awareness of scams and the impact that these can have on people’s lives. This will help our communities to be more vigilant and help to prevent scams that are targeted at older and vulnerable people.

“There is much good work under way to prevent scams, but I believe that more needs to be done to protect people from the callous scammers who blight the lives of many of their victims. It is vital that the opportunities for scammers are removed and that Wales becomes a scam free country.”

In addition to raising awareness about scams and their impact, WASP is also currently developing the UK’s first anti-scammers charter. Due to be launched in the autumn, the charter will help to protect older and vulnerable people across Wales from financial fraud.

Older People’s Commissioner for Wales, Sarah Rochira, said: “Despite much good work across Wales, scams are still a growing issue for older and vulnerable people and can have a devastating impact on their lives.

“By bringing together key organisations across the public, private and third sectors to not only raise awareness within our communities about the nature and impact of scams, but also to develop practical tools like the anti-scammers charter, we can make a real and positive difference that will help to protect older and vulnerable people across Wales from scammers and the crimes they perpetrate.”
Scams Awareness Month July 2015

The Chartered Trading Standards Institute’s Consumer Empowerment Alliance launches Scams Awareness Month on 2 July at the CTSI conference in Bournemouth.

The message this year is to bring the news about scams into the open, to get people talking about different scams, and to help spread the message that scams can be stopped if we all work together. There will be four themes – Telephone scams on week 1, online during week 2 beginning 13 July, mail scams beginning on the 20th and doorstep scams on week 4 from 17 July.

Scams Awareness Month is all about creating a self-supporting network of confident, alert, consumers. People ready, willing and able to spot scams. It’s about people refusing to be rushed into taking decisions they will later regret; and it’s about them refusing to be silenced by a sense of shame or weary acceptance.

Whether you’re an individual consumer looking to protect yourself and family from scams or an organisation or group representing consumers, your efforts during Scams Awareness Month 2015 are important because they will help spread the message that scams can be tackled if we take our time to spot the signs and share what we learn with others.

Scams: Don’t be rushed, don’t be hushed...

Free resources can be ordered on the CAB website as well as a pack containing ideas for events that you can organise. Posters, postcards and bank information can be downloaded for use on your website, or you can order copies to hand out at events. Why not consider joining up with your local Trading Standards department to organise something? If you’re using social media use #ScamAware.

Citizens Advice - Scams Awareness Month

In this issue, we will look at the four themes focused on during Scams Awareness Month which are; telephone, online, mail and doorstep scams.

Telephone scams

Bank phone scam

Fraudsters pretending to be bank officials is now the most prevalent phone scam. There have been fresh warnings about a fast-growing phone scam where fraudsters pose as bank staff in a bid to con us out of money.

Some £23.6 million was lost in 2014 because of this, says advice body Financial Fraud Action UK (FFA UK). It says the con is now the most widespread phone scam in the UK.

How it works

While there are variations of this phone scam, the fraud typically works with the criminal calling the victim and pretending to be from their bank.

The fraudster will then convince the victim that fraud has been detected on their account and they need to act fast to protect their money by moving it into a ‘safe account’, or risk losing it all. The con is often successful because criminals use techniques, such as ‘spoofing’ the telephone number on a person’s caller ID so it matches their bank’s number, or referencing genuine account information which they have fraudulently obtained elsewhere.
Raising awareness

The data has prompted the Neighbourhood Watch (NHW) network to make the issue the focus of its national awareness week.

NHW's 173,000 volunteers in England and Wales will tell residents in their local areas to "hang up on fraud". They will ask neighbours to share warnings and pass on advice to three of their friends. It's hoped this way more than two million people will be reached by the end of the campaign.

How to protect yourself

Here are some tips on how to avoid this being conned out of your money through a phone scam.

- Be wary of unsolicited phone calls and especially cold callers who suggest you hang up and call them back. Fraudsters can keep your phone line open by not putting down the receiver at their end.
- If you feel something is suspicious, hang up, wait five minutes to clear the line, or where possible use a different phone line to call your bank or card issuer on their advertised number.
- If you don't have another telephone to use, call someone you know first to make sure the telephone line is free.
- Remember your bank will never ask you to check the number showing on your telephone display matches their registered telephone number. The display can't be trusted.
- Bear in mind criminals may already have basic information about you, like your name, address and account details, so don't assume a caller is genuine based on these.
- Never tell anyone, including the bank or police, your four-digit PIN, your password or online banking codes and any personal detail unless you are sure who you are talking to.

If you're being contacted by cold callers, visit BT's Unwanted Calls website for useful information on how to screen or block telephone calls. The website also has useful links to organisations hoping to raise awareness and encourage people to manage and report unwanted calls and texts.

It's also important to remember that your bank and the police will never:

- ask for your four-digit card Pin or online banking password, even by tapping them into the telephone keypad;
- ask you to withdraw money to hand over for safekeeping;
- ask you to transfer money to a new account for fraud reasons, even if they say it is in your name;
- send someone to collect your cash, Pin, payment card or cheque book if you are a victim of fraud;
- ask you to purchase goods using your card and then hand them over for safe-keeping.

If you fall victim to fraud or even if you're unsure contact your bank and tell them what has happened. You should report the crime to the police through Action Fraud by calling 0300 123 2040.
Warning about fraudsters sending fake bank text messages

A new scam is doing the rounds, involving 'spoof' text messages.

An anti-fraud group is warning of a new scam where fraudsters try to trick people into revealing their bank account details by sending a series of text messages purporting to be from their bank. The texts claim the recipient's account or account details need to be updated.

They encourage people to call a number or visit a website stating that the matter is urgent. What the recipient doesn't know is that the number or website is controlled by the fraudster, allowing them to steal security details which can then be used to access the recipient's bank account to steal money.

Scammers use specialist software which alters the sender ID on the message so that it appears as the name of the victim's bank, adding it to any existing message threads on the recipient's phone.

The texts warn that the victim will soon get a call from, ironically, the bank's fraud department. Again, it's the fraudster controlling the call and tricking the victim into handing over their security details.

Fraudsters are also sending scam texts which appear to be from a landline number, asking the victim to call their bank. It's hoped that the victim will call the number it came from (the fraudster's) rather than the bank's customer service line.

How to avoid this text scam

Financial Fraud Action UK has some advice to avoid falling victim to this scam.

- As always, be suspicious of any text message that asks you to make transactions or provide sensitive personal information and passwords.
- If you're asked to call the number given in a text message and the number is unknown or suspicious, call your bank on a number you trust to check whether or not the message is legitimate.
- Don't call the phone number a text has been sent from. Call the bank on a number you trust.

BT online

Online scams

Online scam pretending to be from 'Apple pay'

Fraudsters are targeting classified advertisement websites like AutoTrader to advertise vehicles for sale. Buyers are then contacting these 'sellers' to find out more about the vehicles and are being told to pay for them via 'Apple Pay'. In this case the fraudsters are not using the genuine Apple Pay service and potential victims pay money directly to bank accounts in control of the fraudsters. Individuals receive emails claiming to be from Apple Pay with a web link to a cloned website with false terms and conditions of the 'escrow' service. Any money remitted to the fraudsters is then unrecoverable and the vehicles are not delivered.
Protect yourself:
- meet the seller ‘face to face’ and view the vehicle before parting with any money.
- be cautious of web links in an email. They may not direct you to the genuine website.
- report scam advertisements to the classified advertisement websites.
- if the vehicle is below market value, consider whether this is an opportunity too good to be true!

Email scam pretending to be from the Royal Mail

A scam email is currently being sent to victims fraudulently claiming to be from the Royal Mail. Attached to the email is the CryptoLocker virus.

The victim receives an email purporting to be from the Royal Mail stating that they are holding a parcel/letter for the victim. The victim is then required to contact the Royal Mail to arrange for the item to be resent/collected.

By following the instructions within the email the CryptoLocker virus is subsequently downloaded to the victim’s computer. This virus encrypts files on the victim’s system and requests a ransom be paid in order for the files to be decrypted.

Additional incentive is added for early repayment as the ransomware states that the cost of decrypting the files will increase the longer the fine is outstanding.

Protect yourself:
- look at who the email is addressed to. Is it generic or specifically addressed?
- look at the quality of the images included on the email. Are they of sufficient high quality that they could come from Royal Mail?
- do not open attachments from unsolicited emails regardless of who they are from.
- do not click on the link supplied. Instead, go to the relevant website and log in from there.
- check the address of any email received to see if it appears legitimate.

If you believe that you have been a victim of fraud you can report it online http://www.actionfraud.police.uk/report_fraud or by telephone 0300 123 2040.

Flight ticket abroad fraud

People looking for cheap flight tickets are being targeted by fraudsters. New websites are continuously being created with slight changes to the company names with the intention to deceive the public. They offer tickets at bargain prices and usually request for payment via bank transfer. These tickets do not materialize and the funds are retained by the fraudsters.

Protect yourself:
- where possible, buy from well-known company names. If you've never heard of a company, conduct some due diligence.
- use the internet. Type the name of the company/site you are buying from and look for reviews of what others customers are saying about the company. Bad customer service feedback usually finds their way online quite quickly.
- use companies that are ATOL or ABTA Registered. You can check this here: http://abta.com/go-travel/before-you-travel/find-a-member or http://www.caa.co.uk/application.aspx?catid=490&pagetype=65&appid=2
Mail scams

Scams can come to you by phone, email or post. There are many different types of scams, such as fake lotteries and prize draws, get-rich-quick schemes, bogus health cures, investment scams and pyramid selling, to name just a few. It’s important to note there is a difference between scam mail and legitimate mail sent by companies to advertise lawful services or the sale of genuine goods. Scam mail is sent for the sole intention of obtaining money through deception and/or fraud.

Royal Mail is bound by the Universal Service Obligation and is required by law to deliver all mail entrusted to it. However, Royal Mail are determined to do all they can to prevent scam mail entering the postal system with the help of their customers. Royal Mail want to know about potentially fraudulent mail so that they can work with the relevant authorities who can then investigate and take action.

Royal Mail and Trading Standards have joined forces to launch a new initiative to tackle scam mail in the postal system. Find out more about the scam mail initiative here.

What to do

If you think you or a family member is receiving scam mail, you can report it to the Royal Mail. If you have received items of mail you believe to be from fraudsters please send them to the Royal Mail, with a covering letter to:

FREEPOST SCAM MAIL

You can also email at scam.mail@royalmail.com or report your concerns by calling 03456 113 413. Royal Mail will send you a scam mail report form for completion together with a prepaid addressed envelope in which to return the form with examples of the scam mail received.

Alternatively, you can contact Citizens Advice consumer service by calling 03454 04 05 06, writing to Citizens Advice consumer service, Post Point 24, Town Hall, Walliscote Grove Road, Weston Super Mare, North Somerset, BS23 1UJ

If you’re moving home Action Fraud recommends that to reduce the risk of identity fraud you should use Royal Mail’s Redirection service to redirect mail from your old address to your new address for at least a year. If you hold power of attorney for somebody who you believe is a victim or vulnerable to being a victim of scam mail you can apply on their behalf for a Redirection of mail at a Post Office® branch or by post.

If you believe that you have been a victim of fraud you can report it online http://www.actionfraud.police.uk/report_fraud or by telephone 0300 123 2040.

Security - What to do about scam mail | Royal Mail Group Ltd
Clairvoyant scams

Psychic and clairvoyant scams happen when a fraudster approaches you to tell you they have seen something either wonderful or terrible in your future. They ask for money in order to provide a full report about it.

The apparently psychic or clairvoyant fraudsters approach their victims by email, post, telephone call or even face-to-face.

They may tell you that you are in some kind of trouble, but can offer a solution in return for payment. They may claim to be able to give you winning lottery numbers, or offer to remove a curse. The fraudsters tend to ask for an administration fee for their services. Fraud has been committed if money has been lost.

If fraud has been committed, report it to Action Fraud.

Grandmother, 69, fleeced out of £20,000 life savings by string of mail scams was found on 'sucker list' used by fraudsters

A 69 year old grandmother told how she was fleeced out of £20,000 of her life savings by a string of mail scams. Widow Randi Lane's name was found on a 'sucker list' used by fraudsters after a raid on a distribution house from where the letters are sent. But before the discovery she had lost tens of thousands of pounds replying to scam letters from lotteries and so-called clairvoyants.

The trusting grandmother-of-two said she feels like she has been taken for a fool by the 'terrible' scammers who have deliberately targeted her with up to 20 letters a day.

Mrs Lane - who moved to England from Norway almost 50 years ago - began receiving the abundance of mail when she moved into her current home St Annes, Lancashire, in 2006. And over the nine years since she has forked out as much as £20,000 - paying between £20 and £40 a time to supposed mediums and lottery schemes promising prizes of millions of pounds.

Mrs Lane's was one of dozens of names found on a 'suckers list' when the National Scam Hub raided a distribution house from where scam mail would be sent. Trading Standards bosses said the case was an example of con artists using cleverly-worded letters to groom people into handing over their hard-earned cash. The widow, whose name was found on a suckers list, receives up to 20 scam letters each day.

A spokesperson from Trading Standards said: 'Mrs Lane was highlighted to us as being on what they call a 'sucker list'.

'Unfortunately, particularly with elderly, vulnerable people they can be taken in and it can open up the flood gates. These people are effectively groomed. A more sinister development is a clairvoyant saying they can see a big money win. Surprise, surprise, the victim then gets a letter from the lottery. And they personalise letters using their first names - it's a very vindictive way of earning a living.'

But despite stopping replying to the letters last year, Mrs Lane still gets up to half a dozen letters every day as well as several phone calls.

She said: 'These people normally target people who are elderly or alone or don't get out much. They take advantage of vulnerable people - it is terrible.

'But if I can stop just one person from doing what I have done, and stop more people from being hoodwinked, I am willing to share my story.'
Doorstep scams

Door-to-door frauds can take many forms, including:

- pressure selling
- unfair contracts
- overpriced or substandard home maintenance or improvements
- phoney consumer surveys
- bogus charity collections.

Such frauds involve promoting goods or services that are either never delivered to you or are of a very poor quality. Fraudsters may also bill you for work that you didn't agree to. There are specific laws about door-to-door sales. Many are required to give you a ‘cooling-off’ period (where you can change your mind or request your money back). Bogus tradesmen will offer none of these, and even if they do, you can be sure their ‘guarantee’ will not be honoured.

Bogus salespeople will provide false identity or contact information, making it impossible for you to identify or contact them. If you've paid them in advance, you won't get your money back.

Even if your bank or insurance policy covers any loss, you'll still have to contend with a damaged credit rating, continued correspondence over a prolonged period to repair the damage, and the emotional distress and anxiety identity theft can cause.

Also, be wary of opening your door to a potential burglar or someone who wants to get inside your property to enable other people to break in. Once they get through your door, fraudulent salespeople can take note of your valuables and any security measures you have in place.

Are you a victim of bogus tradesmen fraud?

- You've bought faulty, overpriced or substandard goods or services from someone knocking at your door.
- You've paid for these goods or services by credit or debit card.

What should you do if you've been a victim of bogus tradesmen fraud?

- Report it to Action Fraud.
- You can report the salesperson to by calling 08454 04 05 06 or to your local Trading Standards Authority if you believe they have sold you faulty, inferior or overpriced products or services.
- Similarly, you can seek advice from the Citizens Advice Bureau about the terms and conditions of any agreement or contract you may have signed.
- If you've made the payment by credit/debit card or by cheque, contact your credit card company and/or bank and advise them that you’re a victim of improper door-to-door sales techniques and your identity or financial details may have been compromised. They’ll advise you on cancelling payments and ensuring your finances remain secure.

Advice to protect against bogus tradesmen fraud

- Always ask for identification before letting anyone you don't know into your house.
- Check credentials, including a permanent business address and landline telephone number. The mobile phone numbers given on business cards are often pay-as-you-go numbers which are virtually impossible to trace.
• Take control by asking the questions. Ask for references from previous customers or to see examples of their work.
• Don’t sign on the spot – shop around. Get at least three written quotes to make sure you’re not being ripped off.
• If in any doubt, ask the person to leave or call Citizens Advice on 03454 04 05 06.
• If you’re suspicious, why not ask the salesman if you can take their photograph – on your mobile phone, for example? If the person is legitimate, they probably won’t mind.

If you do decide to buy:
• always get any agreement you make in writing
• beware when filling in forms or when speaking to the salesperson, that you don’t reveal confidential details that a fraudster could use to assume your identity or take control of your finances. This may allow a fraudster to steal money from your account or order goods and services in your name
• usually, you have a seven-day cooling off period. So if you decide to cancel the contract, act fast think very carefully about having any work done or goods delivered during the cooling off period. You may have to pay, even if you change your mind.
• never pay for work before it has been completed, and only then if you are happy with it.
• Legitimate doorstep selling involves someone selling you goods or services in your home or on your doorstep. Many honest businesses use this technique – but so do fraudsters.
• Buying on your doorstep can be convenient. However, a salesman who uses clever tactics can pressurise you into buying something you actually don’t want or something that’s poor value for money.

To report a fraud and receive a police crime reference number, call Action Fraud on 0300 123 2040 or use our online fraud reporting tool.

To mark Scams Awareness month, Age Cymru Powys are inviting people to their “Come and Meet” open morning on Tuesday 7 July 2015

This is a great opportunity to have a drink and meet the staff. We would really like to hear about your experiences or concerns and whilst you could gain some really valuable information on how to recognise and protect yourself from scams.

Did you know that ...

• 380,000 people each year fall victim to prize draw scams
• Office of Fair Trading research estimates that UK consumers lose about £3.5 billion to scams each year
• A large proportion of victims are older people in the first stages of memory loss

So join us on 7 July 10am - 12pm at
Age Cymru Powys
11&12 Severn Street
Newtown
Powys

For further information or if you would like to speak to a member of staff please call 01686 623 707
What to do if you think you've been scammed

Useful contact numbers
- Police (non emergency)     101
- Trading Standards via Citizens Advice Bureau 03454 040506 (English) 03454 040505 (Welsh)
- Action Fraud       0300 123 2040
- Mail Preference Service     0845 703 4599
- Telephone Preference Service 0845 070 0707
- Age Cymru advice line     08000 223 444

If you would like to share with us any information on scams, please email us at scamsawareness@agecymru.org.uk

Stop! Think twice, seek advice, say NO to scams!!

Scams checklist
If an exciting offer seems too good to be true, think about the following warning signs and ask yourself if it is a scam:
- was the offer unsolicited?
- do you have to respond quickly? What's the rush?
- do you have to pay for a prize or ‘free’ gift?
- do you have to ring a premium rate number (one starting with ‘09’)?
- are you being asked for your bank or credit card details?
- is the business reluctant to give you its address or contact details?
- are you being asked to keep the offer confidential?

Always stop, think and be sceptical before signing anything or handing over any money.

If the worst happens and you are a victim of a scam, or if you want advice on how to protect yourself, contact Action Fraud Tel: 0300 123 2040 (national rate) for help.

Please click on this link to download our Information card Age Cymru Information card
And also our scams door hanger Age Cymru Scams doorhanger

What to do if you think you’ve been scammed

Useful contact numbers
- Police (non emergency)     101
- Trading Standards via Citizens Advice Bureau 03454 040506 (English) 03454 040505 (Welsh)
- Action Fraud       0300 123 2040
- Mail Preference Service     0845 703 4599
- Telephone Preference Service 0845 070 0707
- Age Cymru advice line     08000 223 444

If you would like to share with us any information on scams, please email us at scamsawareness@agecymru.org.uk

Stop! Think twice, seek advice, say NO to scams!!