

Powys Trading Standards

Consumer Fraud Team – Scam Presentation

Nikki Davies Wheeler
Senior Trading Standards Officer
Tel No: 01874 623420
Email: nikki.davies-wheeler@powys.gov.uk
Neuadd Brycheiniog
Cambrian Way.
Brecon
Powys
LD3 7HR





Our work with adults in need of care /support in the fair trading environment

- Protect consumers from becoming victims of crime utilising our doorstep rapid response system
- Setting up No Cold Calling Zones
- Work with Police, Social Care, banks and the Court system
- We actively prosecute rogue traders who target vulnerable consumers
- We support victims of financial abuse (scams)- with reassurance, education and removal of scam mail/products



What is a scam??? It's a FRAUD – criminal activity and financial abuse.

Designed to persuade consumers to part with their money.

Usually offering a win or prize – neither of which exist.

Offering "miracle" products that may be unsafe.

Offering "exclusive or luxury" products that aren't!

Offering a link to a dearly departed relative via clairvoyance, mediumship etc.

Offering a relationship – by email, Facebook, Skype

All of the above for a "reasonable" fee !! Can be by post, phone or email.

What is a Scam?

- A Scam is a scheme to con people out of their money. Other names for a scam include fraud, hoax, con, swindle, cheat.
- Each year millions of people in the UK fall prey to scammers.
- Estimates put the total cost to consumers at £73 billion with losses to massmarketed scams alone of £5 billion.
- Most victims don't report scams Surveys Have found reporting levels as low as 5 per cent.
- The impacts are huge: some people lose their life savings. But victims also suffer emotional trauma, can become depressed, lose the confidence to live independently and can suffer long-term health problems as a result.





















Who is a scam victim?















Search

Cymraeg



Citizens Advice Choosing an approved trader Scams and Scam Mailings Community Messaging

Doorstep crime and rouge traders

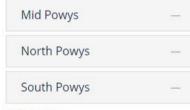
Scam artists set out to get you to part with your cash. Everyone should be on their guard as scammers are very sophisticated at fooling people that what they are offering is legitimate.

The following are typical scams:

- Letters from psychics or clairvoyants promising to make predictions that will alter your fortunes for a fee.
 Sometimes they threaten that bad things will happen if you don't respond.
- 'Phishing' for your identity, such scammers ask for your personal account details claiming that they are from a
 legitimate business you deal with. They will use your details to take money from your account or to buy luxury items
 on your account.
- Bogus holiday clubs offer a free luxury holiday but you may have to pay for flights, meals and other add ons. You
 may be subjected to a long presentation to sell you an unwanted timeshare deal.
- Pyramid selling/gifting schemes where you are asked to pay a fee and sign up new members. Such schemes offer
 rich rewards once you have recruited enough members. These schemes are always illegal; people have lost thousands
 waiting for the promised payout.
- Lotteries, sweepstakes and competitions that promise you have won something but you must send an
 "administration" fee first. These scammers make their money from the fees people send. Beware of mobile phone calls
 like this, as ringing the number they ask you to will cost a fortune on your next bill.
- Unwanted SMS (text) services on your mobile phone. Check all terms and conditions carefully you should not be charged for a text service unless you have agreed to it. Text STOP to the number and the service should cease.
- Foreign money scams and advance fee scams offer you a large sum of money to do something apparently minor like send off a small fee. They may claim that they are trying to get money out of their country, that you have been left money in a foreign will or that you have been awarded a large loan at favourable rates. You will never see the money you send off again.
- Work from home opportunities advertise paid work from home with exaggerated claims about how much you can
 make. They will ask for money up front to buy supplies or to reveal the "secret". Never reply to any such advert that
 asks for money up front.
- Online dating offering a dream partner from overseas. A conversation may start up with the dream partner.
 Eventually they will start to ask you for money for such things as their education, their poor family or to pay for a flight to come and visit you.
- Golden investment opportunities will offer the opportunity to put your money into a sure fire scheme to make
 money by investing in such things as shares, wine, gemstones and other rare items. The items they offer will be
 expensive, very high risk and difficult to sell.
- . Miracle health cures that promise instant cures from such things and hair loss, arthritis, weight gain etc.



Contact



Call charges











♣ Sign In

Search

Cymraeg



What you can do

Be vigilant for anything that offers a get rich quick deal, intimidates you, asks you to part with money up front, or asks for your personal details. Remember that if it seems to good to be true, it probably is.

Consider registering your details, or those of anyone you care for, with the Mailing Preference Service and the Telephone Preference Service to reduce unwanted mail and telesales calls. Removing your telephone number from the directory (becoming ex directory) may also help.

Report scam emails and phishing attempts to your Internet Service Provider and consider installing antispam software on your computer.

Reporting a scam

If you or someone you know has become a victim of a scam, you will need to report it to Citizens Advice

Consumer Services who will then refer any cases to us that require further investigation. You can also report scams or suspected scams to Action Fraud on 0300 123 2040 or by visiting www.actionfraud.police.uk

Your comments & feedback



Strong communities in the green heart of Wales

ABOUT THIS SITE

Cookies
Terms & Conditions

CONNECT WITH US







GET IN TOUCH

There are many ways to contact the council, click the button below for more details

Contact Us

Different Types of Scams

- Prizes and lotteries
- Email Scams
- Cold Callers
- Scam Mail
- Employment related scams
- Door to Door
- Online Dating Scams













Prizes and lotteries Scams

What it is

- When you're told you've won a lottery jackpot or prize draw to tempt you to steal your details or hand over an advance fee to release the winnings.
- The lottery and prize money doesn't exist, or fraudsters pretend to be a genuine lottery.
- Protect yourself
- Don't respond to competitions you haven't entered.
- Break all contact and alert your bank
- Never reveal your bank details or pay fees in advance to release your prize.
- Spot the signs
- If you haven't bought a ticket, you can't possibly have won.
- You're told to keep your win a secret and to reply quickly or risk losing your winnings.
- You have to pay costs such as taxes, legal and banking fees to release your winnings.











How it happens

- You get a letter or email saying that you've won a jackpot in a UK or overseas lottery.
- It asks you to contact someone who claims to be an official at the lottery company so that you can process the payment of your winnings.
- If you respond, you'll be asked to supply personal information and copies of documents such as your passport as proof of identity. The fraudsters can then use this information to steal your identity.
- You may also be asked to pay a fee to process your claim. Each time you
 pay, you'll be given reasons why your winnings can't be paid out unless you
 make another payment. They'll also give you reasons why the fees can't be
 taken out of your winnings and have to be paid up front. Genuine lotteries
 never ask for money up front to release your winnings.
- You may also be asked for your bank details, saying they will pay your winnings directly into your bank account. But if you hand over your bank details, the fraudsters may use them to empty your account.
- How to report it, Report it to us online or call 0300 123 2040.
- http://www.actionfraud.police.uk/fraud_protection/lottery_fraud











Email Scams

Bank email scams

- These scam emails are from fraudsters who send convincing unsolicited emails that pretend to be from your bank or from a trusted establishment, such as the Financial Conduct Authority.
- Bank scam emails often say there's a problem with your account, and ask you
 to update your bank details, either by email or by clicking on a link.
- A recent survey of 980 Which? members revealed two thirds had a scam email delivered to their inbox, falsely claiming to be from a bank or social networking site.
- A further one in ten had reason to believe they'd received a scam communication, but weren't certain.
- Barclays topped the list of financial institutions being impersonated by fraudsters, with 36% of respondents having received a scam email claiming to be from them.
- Fake Lloyds TSB emails were sent to 35% of respondents, while 31% received false Santander emails and 30% received an email impersonating Halifax and HSBC respectively.











iTunes invoice

Apple customers were targeted by an iTunes invoice phishing scam designed to get them to click onto a link and claim a refund for a purchase that they didn't make. Once their Apple ID and password were typed in, victims were prompted to send over their credit or debit card information.

HMRC tax refund scam

Fraudsters target victims by sending an email claiming that they're due a tax rebate, to try and trick them into handing over their bank account or credit card details. You can read more about the vishing equivalent of this scam

Suspended credit card account or suspended Tesco Bank account

Fraudsters know that any correspondence to do with your credit or bank account can instantly grab your attention – that's why they use this as the focus of many of their scams. As part of this, you're sent a message claiming that something's wrong with your account and prompted to sign into it through a provided link. The link directs you to a fake website that will compromise your details as soon as you enter them.











Cold Callers

- There are a few things you can do to help in the fight against those pesky spam calls, to stop them from reaching you. Register with the Telephone Preference Service
- If you don't want to receive marketing calls, sign up your home phone and mobile to the Telephone Preference Service (TPS). It takes about 28 days for calls to stop.
- It's then illegal for firms in the UK and the rest of the EU to call those who've registered, unless you'd opted in to receive them (including if you ticked the often confusing "allow third parties to contact me" box when filling in an online form).
- TPS may also stop distressing calls intended for a deceased relative.
- How to add your number to the register depends on if it's a mobile or landline:
- Landlines. Add your landline number via the TPS website, or by calling 0345 070 0707 (it costs the same as a standard landline).
- Mobiles. Text 'TPS' and your email address (required to verify your identity) to 85095. TPS insist that the text is free, though some might get a message saying they may be charged up to 15p see the Spam calls MSE News story. Alternatively, you can sign up online or by calling 0345 070 0707.
- http://www.moneysavingexpert.com/phones/no-more-junk













Powys TSD is working with national team to stamp out scams – with the focus being on mail scams

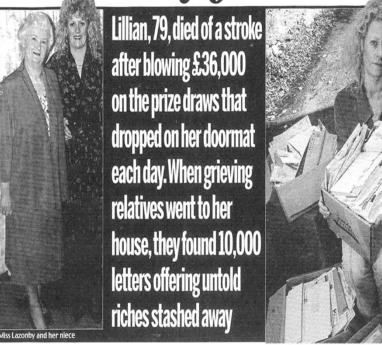
NATIONAL TRADING STANDARDS

Scams Team

Scam Mail



ROGUE TRADERS RUIN LIVES Killed by junk mail















Dealing with scam mail becomes an obsession, a way of life





Scam Mail

- Scams are schemes to con you out of your money, usually by post, phone, email.
- There are hundreds of scams fake lotteries, prize draws, investment scams, get rich quick schemes.....
- Scams target people of all backgrounds, ages and income levels

What we do?

- Hub visits
- Joint enforcement
- Victim Support / Age UK
- Press / Awareness Raising
- Education
- Intelligence sharing



This is all from one victim





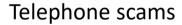












- Investment scams
- Technical Support scams
- Bank account courier scams



Online scams

- Phishing emails
- Dating scams
- Social media scams
- Survey scams



Doorstep scams

- Rogue Traders
- Bogus
 Officials
- Fake charity collections

Employment related scams

"You place your CV or personal details on internet job sites so that potential employers can see them and, hopefully, offer you a job. You're contacted by someone claiming to be an employer or an employer's agent to say they are considering you for a position. You're asked to fill in a questionnaire and may be interviewed over the phone. You may also be referred to the employer's website for further information. Eventually, you're told that you've been successful and the job is yours. Once you have received the job offer, the fraudsters will contact you about arrangements. If the job is abroad, they will talk about arranging travel, accommodation and visas. You'll be referred to an agency that, again, may have a website to give it credibility.

The agency is supposed to help you with all your arrangements – for a fee. When you pay one fee (eg: a visa administration fee), the agency will tell you about another fee that has to be paid (eg: a deposit on accommodation). In reality, the fraudulent agency makes none of these arrangements. What's more, the fraudsters may also ask for your bank account details to set up salary payments. They will use these details to steal money from your account. Some employment fraudsters ask the applicant to pay a fee in order to apply for a job. In reality, there is no job and any fees paid go straight to the fraudsters. Victims may already have given up their previous job and made new accommodation arrangements."

- Action Fraud

https://www.actionfraud.police.uk/fraud-az-recruitment-scams











Doorstep callers

- Legitimate trader?
- Rogue trader?
- Distraction burglar?



Door to Door Scams

- Scammers commonly target older people for doorstep scams. In fact, 85% of victims
 of doorstep scams are aged 65 and over according to National Trading Standards.
 We'll show you some simple steps that you can take to help you stay safe on your
 doorstep.
- Doorstep scams are when someone comes to your door with the aim of scamming you out of your money or trying to gain access to your home to steal items from inside.
- While there are many legitimate tradespeople and officials, it's wise to be on your guard when you answer your door. Doorstep scammers can be pushy and persuasive and it can be easy to fall victim. It's especially important to be vigilant and aware if you live on your own.
 - Age UK

http://www.ageuk.org.uk/home-and-care/home-safety-and-security/doorstep-scams/doorstep-scams/











No Cold Calling Zones

- A No Cold Calling Control Zone is an area in which residents have stated they do not wish to receive unsolicited visits to their homes (cold calls) from businesses
- Zones are selected on the basis of risk and local resident demand/enthusiasm. Also Police and Trading Standards crime statistics are examined and the demographics of proposed areas are sought. Before any zone is launched local residents and businesses are fully consulted to ascertain their views

Online Dating Scams



Scams not only affect the elderly. Recently there's been a lot of scams with social media, online dating and mobile apps that have affected the younger generation but its not limited to just them. These sort of scams can target anyone one at any age.

"Scammers typically create fake online profiles designed to lure you in. They may use a fictional name, or falsely take on the identities of real, trusted people such as military personnel, aid workers or professionals working abroad...Once they have gained your trust and your defences are down, they will ask you (either subtly or directly) for money, gifts or your banking/credit card details. They may also ask you to send pictures or videos of yourself, possibly of an intimate nature."

- Scamwatch

https://www.scamwatch.gov.au/types-of-scams/dating-romance











App Scams

- Using email, text, phone calls, social media, and now apps, scammers are infiltrating
 everyday routine in any way that they can. With more and more consumers searching for
 content and apps related to shopping, coupons and deals, criminals are luring in
 unsuspecting users with "great" offers on products that are typically very expensive.
- Scammers can do a lot of damage with these types of fake apps -- not only can they steal
 the cash you hand over, but they can also use your personal information to make more
 fraudulent charges, open accounts in your name and do other things that can destroy
 your financial life.

So when it comes to protecting your information and money, there are a few important things to keep in mind!

- If you don't recognize the company name, research the app and company before you
 download it
- If an app appears to be a retailer's official app, check the company's website before you download it!
- Never use a debit card in an app or online
- Check your accounts daily

http://www.clark.com/scammers-fake-shopping-apps-steal-from-consumers











What happens to victims?

- Many become estranged from family/carers.
- They become isolated and secretive.
- They run out of money and end up depending on the state for support – care and housing.
- They become stressed/obsessed/ill and end up depending on the NHS for further health support.



We need to work together to support victims and prevent this fraud and financial abuse of the most vulnerable.

What people can do?

- Keep an eye out for workmen, new work done, regular callers, paperwork & bills
- Scam mail/gifts
- Report scams to Action Fraud on 0300 123 2040
- Get advice –Citizens Advice Consumer Service-03454 04 05 06
- Encourage staff/carers/victims to talk about scams and incidents
- Use and support Dyfed Powys Community Messaging System and look for early warnings
- Support joint training
- POCA Opportunities











What are we doing?

- Training Police Officers & Key Partners
- Training Bank & Building Society employees (Banking Protocol)
- Rogue Trader Operations
- Social Media Posts
- Cold Calling Control Zones
- Working with partners via Consumer Hub
- Dyfed Powys Community Messaging
- Prosecution of Offenders
- Proceeds of Crime Actions Compensation / Confiscation







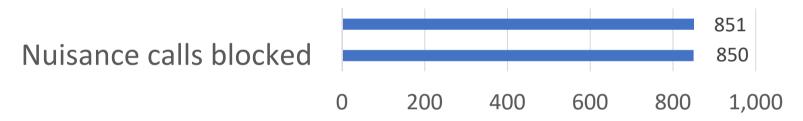




POWYS TRADING STANDARDS CALL BLOCKER PROJECT

4 trueCall nuisance call blocking units have been installed free of charge for vulnerable Powys households since 2017

851 nuisance calls were received by these residents of which 850 were blocked



Since 2017 Powys Trading Standards have installed 4 trueCall units that have received 851 nuisance calls We can estimate that the trueCall units have

- Blocked 161 scam phone calls
- Prevented 1 scam call being successful
- Saved vulnerable Powys households £1,518
- Led to a £1,518 reduction in social care and other costs for the public purse

Total savings so far of £2,279



SO HOW CAN YOU HELP?

Powys Trading Standards
Support Friends Against Scams

What is Friends Against Scams?





Friends Against Scams is a National Trading Standards Scams Team initiative which aims to protect and prevent people from becoming victims of scams by empowering communities to... 'Take a Stand Against Scams.



Raising Awareness with our partners























Thank you for your attention

- If you have further queries, please contact Powys Trading Standards on 01874 623420
- Follow us on Facebook:

https://www.facebook.com/Powys-Trading-Standards-343425435782496/

- Follow us Twitter: @PowysTS
- If you have a consumer complaint, please contact our partners at Citizen's Advice Consumer Helpline on 03454 04 05 06









