



Contents

f h

The Society of Chief Officers of Trading Standards in Scotland have put together this toolkit as a self-help guide to empower our communities to avoid scams and unwanted nuisance sales contact.

An estimated £9 billion is lost to scams annually in the UK. The national position in respect of financial harm is well illustrated in the "WithScotland" briefing on financial harm by the University of Stirling which states;

"Research conducted internationally but also in the UK highlights financial harm as one of the most common forms of elder abuse. Its detrimental effects, impacting both mental and physical health, are far reaching and cannot be overlooked."

There are a number of simple practical solutions you can take to protect you, your family or clients from scams. We urge you to take a proactive approach and implement the safeguards - don't wait until a loss occurs.

We regularly deal with residents who lose their entire life savings to a scam, the consequences can be devastating financially and personally. Sadly statistics show that elderly, vulnerable residents are the most impacted by scams. A number of factors and health related conditions such as dementia can dramatically increase the risks. The loss of a partner is frequently quoted as a reason why a person was caught out by a cruel scam. We can help with a person centred prevention package, available to all residents facing challenges due to health or personal circumstances.

We have extensive feedback from families showing that the packages can dramatically reduce the risk of being scammed and increase a person's

confidence at home.

How to use the tool kit

Select the desired page from our table of contents and click the title to take you straight to the page of interest. More detailed information is available in each section via the click on links or at the listed website.



What is Financial Harm?

Financial harm covers theft, fraud, exploitation, pressure in connection with wills, property, inheritance or financial transactions.

Stopping someone obtaining their money or possessions, or the misuse of someone's property, possessions or welfare benefits. Being scammed by rogue traders or telephone, online, email and postal scams.

What is a scam?

Scams, also known as tricks, cons or swindles - are an illegal act with the sole purpose of getting money from the person they target. Those who commit this crime are usually called scammers, fraudsters or conmen.

In the UK alone the actual figure lost to scams is unknown due to the high levels that go unreported.

Anyone can fall for a scam, regardless of their age or health. However, older people can be at a greater risk of falling for a scam, the risk increases with cognitive decline and dementia can significantly increase the risks of being financially harmed.

Remember someone who lives alone and has limited social contacts may not have anyone they can discuss a letter or a phone call with to work out if it is a scam or not.

This guide will look at various types of scams and offer free practical advice and simple steps to prevent the person you care for from falling for a scam.

Report a scam and prevent more harm

Always report a scam, they can happen to anyone and reporting prevents other people from being harmed.

Doorstep scams

Cold callers offering:

- · Home repairs
- Selling misrepresented goods/services or employing pressure sales tactics
- Claiming to be from an organisation such as your water supplier to gain entry to a home.

Mail scams

- Fake lottery wins
- Bogus health cures
- Investment scams
- · Pyramid schemes.

Telephone & text scams

• The caller claims they are from a bank or other organisation the resident deals with and may sell misrepresented goods and services.

Online scams

 Some fraudsters rely on the internet and email to carry out a wide variety of scams.

Pension & investment scams

Boiler room share and investing frauds.



Financial exploitation

Financial abuse of the elderly is on the rise, and the perpetrator is frequently a family member. Increasing social pressures, fractured families, technological advances, and the use of internet banking all contribute to this issue.

Anyone can be at risk, but age, disability, cognitive impairment and poor mental health may make a person more vulnerable.

Coronavirus scams

The COVID-19 pandemic has been an opportunity for scammers and organised criminals to prey on members of the public, particularly older and vulnerable people who are isolated from family and friends. Some types of scams include:

Fake 'Test and Protect' scams - scammers are using the new Test and Protect as an opportunity to steal your information and money. The NHS says the calls/texts will come from **0300 0135000**, however, scammers can "number spoof" your caller ID. This means that the genuine number could be displayed but the call be may be from a scammer. Contact tracers will not ask for bank details, or payments, or ask you to set up a password or call a premium rate number.

For advice on avoiding Test and Protect scams please or visit:

COVID-19 / Coronavirus testing kits - adverts are appearing on social media, advising consumers of the availability of COVID-19 testing kits. Legitimate medical testing won't be sold door-to-door or through social media advertisements.

For further information on Coronavirus scams or visit:

Online scam awareness session

Complete an online learning session in the comfort of your own home or wherever is convenient! It's quick and interactive, so you will be able to learn about scams in a fun way, enabling you to help spot victims and protect yourself and others!

or visit:

If you would like online training

Scam risk checklist

Answer the following questions to help determine someone's scam risk threat.

	Yes	No
They receive cold calls on the phone or doorstep		
They are socially isolated or have recently been bereaved		
They have been scammed before		
You suspect, or they are diagnosed with having a form of dementia, such as Alzheimer's disease		
They are secretive about finances and have unexplained financial losses		
They can be impulsive due to mental health issues		
They listen to sales chat from cold callers		
They have never signed up for the Telephone or Mail Preference Service or taken steps to block unwanted contacts		
They have a computer and shop online, but aren't always confident		
They employ cold callers to carry out home maintenance work i.e. driveways, gardening		
They have a pension pot or significant finances available		
They don't have access to a list of trusted tradesmen		
They like to donate at the door to charities		
They are generally trusting of people's motives		
They are always receptive to a needy cause		

The more YES answers, the greater the risk of being scammed.

Report a Scam & Prevent more Harm

Anyone can fall for a scam, individuals from all ages, backgrounds and geographical locations. Even large sophisticated businesses have fallen victim.

Dementia and scams

People living with dementia are at an increased risk of serious financial harm if they are not protected with the appropriate safeguards discussed in this guide. Evidence clearly shows that callous organised criminals actively seek to exploit the most vulnerable residents in a community.

Home maintenance crime is a particular problem. Residents should not deal with unverified cold callers offering gutter cleaning, roof repairs, driveways and landscaping etc.



We have assisted

to produce a scam prevention guide for:

- People living with dementia
- · Carers of people living with dementia

For more information

or visit:

Power of Attorney covering financial matters can play a key role in preventing loss and should be a priority. Have a discussion with the bank about the support they can provide to protect a customer with dementia.

Case Study - John's story

The following case study is a real-life example of what has happened to someone living with dementia because of a scam.

How did we help?



Telephone scams & nuisance calls prevention

Nuisance calls and messages are inconvenient and annoying but can also cause considerable distress, anxiety and financial loss for vulnerable consumers. If you are receiving these calls and messages you can:

- Contact your phone provider about call blocking solutions or contact Trading Standards to ask if you qualify for a free call blocker.
- Register with the Telephone Preference Service. This allows consumers to opt out of receiving any unsolicited telesales calls to register or visit:
- Contact OFCOM (the UK's communications regulator) for excellent advice on how to deal with nuisance calls, texts and how to react to unwanted sales calls
 for OFCOM, or visit:
- Try not to panic. Panic is a powerful tool that scammers use to cause irrational thinking.
- Never give out any information. Scammers use this information to build a profile on you.
- If in doubt hang up. Trust your instinct; it's usually right.
- Never give out any bank details. If in doubt visit your local bank in person.
- Scam calls usually have a 1 or 2 second delay before you hear the callers voice.
- Call your phone provider to get a free caller display on your phone.

Call blocker user feedback:

Trading Standards can provide telephone call blockers free of charge, to help residents in vulnerable situations who are experiencing a high number of nuisance calls, or have been a victim of a scam. The unit is provided free of charge on an indefinite loan. Call Blockers has already blocked over 800,000 unwanted calls.

Doorstep crime & Prevention

We work in association with Police Scotland and Adult Protection to keep residents safe from rip off doorstep callers. Every year organised criminals knock doors uninvited and offer to do roof repairs, driveways and gardening work. The price frequently rises from the original quote and the work is rarely done properly, if at all. Unscrupulous salesmen selling goods and services at inflated prices have also caused problems.

A Yellow "No Cold Calling" sticker can be displayed on your door, this gives you the option to say no to uninvited doorstep traders.

for a sample sticker, contact
Trading Standards for more information at:

Key prevention messages:

Charitable donations

Unfortunately, in some circumstances, regular donations to genuine charities can cause financial detriment, especially if the person has had a change in their financial situation. If you are a carer or guardian it may be an idea to check outgoing donations to see if they are still sustainable.

Should you wish to make a complaint regarding the actions of a charity, for example pressure to commit to a direct debit either by phone or at the door, or just to check if they are indeed a legitimate charity, you can do so by contacting the The Scottish Charity Regulator (OSCR) by or visit:



SCOTSS Approved Trader scheme

You can safely choose an Approved Trader, to carry out work in the home. Approved Traders follow a strict code of practice and will not turn up at your property unannounced.

Traders are vetted by Trading Standards and supported by Police Scotland. Help us stamp out doorstep crime.

To find a local trader,

or visit:

Further advice to find a reputable trader:

- Display a No Cold Calling sticker to say no to uninvited doorstep traders
- Get quotes detailing the work as well as the cost
- Make sure they have an established trading address and a land line number
- Check if guarantees are insurance backed
- · Avoid paying cash and always get a receipt
- Don't pay up front
- Don't pay if you are unhappy with the workmanship
- Use Care and Repair if you are over 60 and those with disabilities
- Phone Trading Standards and Report if you think bogus workmen are working in the area. Keep a note of the registration number of the van and any other details.





Scam mail & prevention

Each year mass marketing mail scams, which often target vulnerable or disadvantaged consumers, cost approximately £3.5 billion worth of detriment to UK consumers and seven out of ten older people in the UK are targeted.

In many instances the of scam mail display characteristics similar to brainwashing and can be resistant to help. To view an example please visit:

In these cases advice is unlikely to make a difference and mail redirection and Power of Attorney may be the only way to stop the loss.

There is a difference between and legitimate mail sent by companies to promote lawful services or genuine goods. View an example at:

What to look out for when someone is receiving scam mail:

Reporting scam mail

Scam mail should be reported to Royal Mail by writing to Freepost Scam Mail, calling **0800 0113 466** or by emailing

Prevention Services - Case study



Online scams & prevention

We regularly receive complaints from people who have lost significant sums to fraudsters via internet sites that fail to supply the goods and services offered. It is essential that you understand how to safeguard your purchases and identify legitimate sites.



Password security tips

- Use a different unique password for each of your important accounts.
- Use an eight-character password with numbers, symbols and mixed-case letters is harder to guess because it has 30,000 times as many possible combinations.
- Don't use personal information, common words or phrases.

Transfer money safely online

- Never send money to someone you have not met in person.
- Never send money to pay for 'taxes' or 'processing fees' on lottery or prize winnings.
- Never provide your banking information to people or businesses you do not know.
- Never send money in advance to obtain a loan or credit card.
- Never send money in advance to cover any kind of deposit or fees concerning the sale or purchase of a vehicle.
- Never send money for an emergency situation without verifying that it is a genuine emergency.
- Never send funds from a cheque in your account until it officially clears which could take weeks.
- Never send a money transfer for online purchases.
- Never open an attachment from, or click on a link in an unsolicited email claiming to be from a money transfer service.

Purchasing online

- Make sure your computer has effective anti-virus software.
- Ensure the website has contact details: name, address, phone number and email.
- Look for https:// and the golden padlock to ensure the website is secure.
- Only buy event tickets from authorised outlets, watch out for scam and spoof websites.
- Never give, or send your pin number or passwords to anyone.
- For extra protection use a credit card, if the goods are more than £100 the credit card provider has equal liability for most problems that may arise, i.e. if the trader goes bust you can claim against the credit card. Remember to always pay the balance before interest is added!
- · Avoid sites that do not accept credit cards.
- Always read the terms and conditions don't just tick the box!
- Save or print all paperwork, including site details, descriptions, and the confirmation details.
- If buying from auction sites familiarise yourself with the rules and practices.
- Consumers are generally not liable for fraudulent transactions on their debit or credit card as long as they report any unauthorised use within a reasonable time. Always check your bank statements.
- Use a credit card if you are buying from abroad as it can be extremely difficult to sort out problems if they arise as the laws of the applicable country will apply.
- Counterfeit goods are frequently sold online, only buy from well established, familiar sites.

For more information on how to stay safe online, or visit:



Romance scams

Scammers take advantage of people looking for romantic partners, often via dating websites, apps or social media by pretending to be a prospective companion. They play on emotional triggers to get you to provide money, gifts or personal details. 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.

Dating and romance scammers will express strong emotions for you in a relatively short period of time, and will suggest you move the relationship away from the website to a more private channel, such as phone, email or instant messaging.

Scammers will go to great lengths to gain your interest and trust, such as showering you with loving words, sharing 'personal information' and even sending you gifts. They may take months to build a romance and may even pretend to book flights to visit you, but never actually come.

Once they have gained your trust, they will ask you (either subtly or directly) for money, gifts or your banking/credit card details. Often the scammer will pretend to need the money for some sort of personal emergency like an unwell family member who requires immediate medical attention, or having a failed business that needs bailing out. The scammer may also claim they want to travel to visit you, but cannot afford it unless you are able to lend them money to cover flights or other travel expenses.

The scammer may send you valuable items like laptops or mobile phones, and ask

you to resend them somewhere. They will invent a reason they need you to send the goods or may ask you to buy the goods yourself and send them somewhere. This is

a way for them to cover up their criminal activity, it is very likely to be a form of money laundering which is a criminal offence.

Online dating and romance scams cost millions of pounds every year. The money you send to scammers is almost always impossible to recover and you may feel long-lasting emotional betrayal at the hands of someone you thought loved you.

Report a Scam & Prevent from Harm

National Cyber Security Centre

You can help to play your part in protecting others by reporting suspicious activity online and help make the internet a safer place. or visit:

- Report a scam email here or visit: https://bit.ly/NCSCemailscam Forward suspicious emails to report@phishing.gov.uk.
- Report a scam text here or visit: https://bit.ly/NCSCtextscam
 Forward suspicious text messages for free by forwarding it to 7726.
- Report a scam phone here or visit: https://bit.ly/NCSCphonescam. Call If you've lost money, you can contact your bank and report this to Police Scotland on 101.
- Report a scam website here or visit: https://bit.ly/NCSCwebsitescam. Report a suspicious website link or URL to the NCSC by filling out this online form or visit: https://bit.ly/NCSConlineform.
- Report a scam advert here or visit: https://bit.ly/NCSCadvertscam. If you see
 a suspicious ad in a paid-for space, you can report it to the Advertising Standards
 Authority by clicking here or visit: https://bit.ly/ASAreport.

Sextortion - Email scam

What should I do?

Cyber criminals are sending victims scam emails in a phishing attempt to let them believe they have been filmed on their computer watching porn and demanding payment.

There have been hundreds of reports made from concerned victims who have received these alarming emails which can contain the victim's own genuine and recent password.

The criminals are believed to have obtained the details through a previous data breach.

Sextortion - Blackmail victim

If someone threatens to share explicit images of you unless you pay them money, and you are certain that they do have the images, then you are a victim of sextortion.

What should I do?

Safer banking/financial ombudsman

Banking scams are on the increase. A typical example is a scammer claiming there has been fraud on your bank account and you need to act quickly to protect your money. The solution is to transfer your money to a 'safe account', however the account is controlled by the fraudster and when you move the money, they steal it.

To make their call appear genuine, fraudsters often use a tactic called 'number spoofing'. This enables them to alter the phone number from which they are calling so that it matches your bank's number. They may ask you to check your handset display in an attempt to convince you it's a real call.

Your bank or the Police will never:

- ask you to transfer money to a new account for fraud reasons, even if they say it is in your name;
- phone you to ask for your 4-digit card PIN or your online banking password, even by tapping them into the telephone keypad;
- ask you to withdraw money to hand over to them for safe-keeping;
- send someone to your home 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.

Talk to your bank and ask how they can help safeguard your account from fraud. Look out for any banks who offer fraud refund guarantees.

Financial complaints

Lost money to a scam and can't get a refund?

You can escalate your complaint to the Financial Ombudsman who can give a free, unbiased decision.

In addition, if a business and customer can't resolve a complaint between them, the Financial Ombudsman can decide if someone's been treated unfairly. For more information or to make a free complaint or visit:



Sign up & stay informed

Do you want to receive FREE alerts on potential criminal activity in your community?

The system, run by Neighbourhood Watch Scotland, allows you to stay up to date with the latest news – including reports of doorstep crime, scams and more. Alerts are sent out by email and/or text.

To sign up, or visit:

For more alerts on Coronavirus scams from Trading Standards Scotland please or visit:



Switch & save

You could save hundreds of pounds over the year by switching to a better deal.

What are price comparison websites?

Price comparison websites allow you to compare a whole host of consumer items such as: car/house insurance, broadband, fuel suppliers and even savings on your weekly shop. Simply type "compare" and the product you want to save on into your browser.

Before you start:

- It is best to have details of when your renewal date is due for your current supplier. For car insurance you need details of any penalty points and no claims discount and what your excess is. You should check if you have any penalties to leave your current supplier
- Quality is as important as cost, so focus on getting value for money.
 For example the level of cover and standard of customer service may vary
- Contact your existing product provider to ask if they can match the deal that you have found
- Not all companies are on comparison websites, so search their websites or contact them direct for a quote
- It is important that you carry out a review every year to make sure your current product supplier is remaining competitive.
 Be aware that some deals are discounted for new customers only and rise.

Technology Enabled Care (TEC)

Technology Enabled Care (TEC) is the term to describe how technology can be used to support health and wellbeing. This includes:

Telecare - also known as a community alarm, is a service linking individuals from their own home to the Council's 24-hour call response centre. Telecare provides reassurance and peace of mind to family, friends and carers.

Benefits of Telecare

- Provide 24 hr response to accident or emergency 365 days per year
- · Enable a person to live independently in their own home
- · Help manage safety and security risks
- Enhance fire safety
- · Facilitate safer hospital discharge
- · Reduce hospital admission and injuries
- Additional equipment supplied can sense risks such as smoke, floods and gas, call for help if you fall and remind you to take your pills at the right time.

Telehealth

Telehealth uses Flo, an easy to use text message system design by the NHS. It helps you and your health professional track and or/manage your health and wellbeing for example, your blood sugar or glucose levels.

Benefits of using Flo

- Less time spent waiting for and attending appointments
- Opportunity to understand and take ownership of your own health
- Greater independence
- Stay healthier for longer
- Text messages sent to and from Flo are free.



Power of Attorney

A Power of Attorney is a legal document that features statements called 'powers'. There are three different types of Power of Attorney:

General Power of Attorney (GPA)

Usually created for a set amount of time or for a specific issue.

Continuing Power of Attorney (CPA)

Allows you to appoint someone to look after your financial and property affairs. If you want to authorise someone to act on your behalf whilst you are still capable. The final decisions still lie with you. This can include the powers to manage your bank accounts or sell your house.

Welfare Power of Attorney (WPA)

Enables the attorney to make decisions about your health and welfare but only if you are unable to do this yourself. No-one can make decisions about your welfare whilst you have the ability to do this for yourself.

Nobody has automatic authority to make decisions about your life if you lose the ability to make decisions for yourself, unless there is a Power of Attorney set up in advance. If you have not appointed an attorney, another person would, in most cases, have to go to court to get the authority to act on your behalf.

for more info on Power of Attorney or visit:



Carers & financial abuse

A review for Help the Aged stated 70% of financial abuse is perpetrated by family members.

It also found that 60–80% of financial abuse takes place in the home and 15–20% in residential care.

Reporting financial harm anonymously

The Adult Support and Protection legislation is designed to protect adults at risk who are unable to protect themselves, their property, rights or other interests.

For further assistance call 0800 902 0042

Consumer advice & Trading Standards

Trading Standards will investigate in cases where residents have been scammed.

Further information on Trading Standards can be found by visiting:

If you have any consumer advice enquiries, please call Advice Direct Scotland consumer helpline on **0808 164 6000**. If Advice Direct Scotland are unable to assist they will pass your enquiry to Trading Standards.



for further information on consumer rights

or

Practical steps to keep safe & avoid scams

Use our checklist to safeguard you or someone you care about.

		,	Yes	No
"No Cold Calling"	' sticker displayed on e	external doors		
Access to reputable scheme.	ole tradesmen through or visit:	SCOTTS Approved Trader		
Registered for tel	ephone and mailing p	reference service		
Redirected mail w	where necessary (scam	mail victims)		
Contacted landling options to stop co	ne and mobile provider old calls/texts	to check network		
Contacted Preven call blocking devi		for a free nuisance/scam		
Checked you are	safe and secure online			
Taken the scam a	wareness course			
Asked your bank	how they can protect y	you from financial harm		
Understand the p methods	rotection available via	different payment		
Researched the boot of Attorney	enefits and protection	afforded by a Power		
Know how to rep	ort a scam and seek ac	lvice		
	dementia and cognitive of being scammed	e impairment can		
Asked Prevention prevention packa	Services about a pers ge	on centred scam		
House alarm and sensor fitted	doorstep security chee	cked CCTV motion		
Bogus alarm butt	on fitted			
Telecare (commu	nity alarm) and associa	ited gadgets		
Arranged a fire sa	afety visit			
Informed about lo active and remove	ocal groups and activit e isolation	ies to keep		

Useful contacts

Highland Council Trading Standards

Tel: 01463 644570,

www.highland.gov.uk/info/20000/trading_standards.

NHS Highland Telecare

Tel: 01478 614211

nhshighland.telecare@nhs.scot

NHS Highland Adult Support and Protection

To report an Adult Protection Concern Tel: **0800 902 0042**

www.nhshighland.scot.nhs.uk/services/asc/adultsupport/pages/welcome.aspx

Advice Direct Scotland

Advice on how to resolve your consumer problem.

Tel: 0808 164 6000

www.consumeradvice.scot

Age Scotland

Information, friendship and advice to older people, their relatives and carers.

Helpline: 0800 124 4222 www.agescotland.org.uk

Alzheimer Scotland

Leading dementia organisation in Scotland.

Helpline: 0808 808 3000

www.alzscot.org/

Get Safe Online

Free Expert Advice on online safety www.getsafeonline.org/

Mail Preference Service

Free opt-out register for unsolicited sales and marketing mail by post.

Tel: 0207 291 3310 www.mpsonline.org.uk

National Trading Standards (NTS)

Protecting consumers and safeguarding businesses throughout the UK. www.nationaltradingstandards.uk

OFCOM

Regulator for communication services like broadband, home and mobile services and TV.

Tel: 0300 123 3333 www.ofcom.org.uk

Office of Public Guardian

Set up or register a Power of Attorney.

Tel: 0132 467 8398

www.publicguardian-scotland.gov.uk/power-of-attorney

OFGEM

Office of Gas and Electricity Markets. Our aim is to protect the interests of existing and future electricity and gas consumers.

www.ofgem.gov.uk

Pension Wise

Free and impartial government advice agency on your pension options.

Tel: 0800 138 3944

www.pensionwise.gov.uk

Police Scotland

Scotland's national police force.
Tel: 101 or 999 in an emergency www.scotland.police.uk

Telephone Preference Service

Free opt-out service for unsolicited sales and marketing calls.

Tel: 0845 070 0707 www.tpsonline.org.uk

The Think Jessica Campaign

Campaign against scam mail. www.thinkjessica.com

Trading Standards Scotland

Scotland's national team who can coordinate and enforce cross boundary cases as well as tackling illegal money lending and e-crime.

www.tsscot.co.uk

Royal Mail

Report any scam mail that has been received in the post.

Telephone: 0345 611 3413

www.royalmail.com

Victim Support Scotland

Provides support to victims and witnesses of crime in Scotland.

Tel: 0345 603 9213

www.victimsupportsco.org.uk





Case Study - John's story

John is a proud, retired professional who is living independently with dementia. His wife died several years ago and his only daughter live 30 miles away. A home carer arrived at the home one day and noted that three men were working on the roof of his property, it transpired they had cold called having noticed a loose roof tile from the road.

They initially quoted £80 but had since claimed that the roof needed emergency repairs and the cost had rocketed to £7,500. John was upset and confused and indicated he just wanted to pay the men to get them away as he felt threatened and embarrassed. The home carer contacted the Police and Trading Standards. The alleged workmen left when they realised that the Police were investigating.

Trading Standards then visited John to give him advice on avoiding scammers in future. It transpires that John was also being targeted by scammers on the phone and through large amounts of mail claiming he had won various prizes. Sadly, John had responded to a large number of fraudsters and over £100,000 of his savings had been withdrawn from his account to pay scammers from all over the world.

Trading Standards raised an Adult Protection alert and a case conference was held to look at the best way to safeguard John.





• John has joined a local supported art class and feels less isolated.

John has lost no more money to scams and his anxiety levels are drastically reduced. His daughter is also more confident in John's ability to maintain independent living.



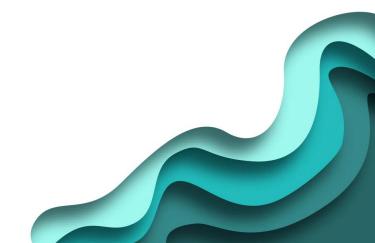


Call blocker user feedback

"The system is wonderful – we appreciate having it immensely. Your team are superb. My wife and I are so grateful to have the call blocker and hugely appreciate having it in our home. Enormous thanks to the council."

"I have arthritis and it takes me a while to answer the phone or door. I can't thank you for the help that you have given and it does make me feel safer. You do good things for us old people and I thank you all."

"Have nothing but praise to East Renfrewshire Council for the equipment. When the phone rings now I know it will be from someone genuine and not from nuisance callers from morning to night. I've got great peace of mind now and relief. The blocker has been of great value to me."





Key prevention messages

- · Display a "No Cold Calling" sticker
- Keep a list of Council vetted Approved Traders
- Keep front and back doors locked
- Use a door chain or bar, genuine callers expect you to be careful
- If you have a Telecare alarm you can ask for a free bogus caller alert button
- Only let callers in if they have an appointment and you have confirmed they are genuine
- Always ask for ID
- Don't keep large sums of money at home
- Ensure your doors and windows are locked
- Look out for those in your community
- Report any suspicious activity immediately on 101
- Call 999 and ask for the Police if you think you are being intimidated or scammed by a doorstep caller.

For further information on doorstep crime and cold callers contact: **01463 664570**



Scam mail through the post

- Mail is being received for lottery winnings, prize draws, health products, charities, clairvoyance, jewellery etc
- The mail is designed to look official and authentic.
 It uses well known marketing ploys which make the content highly persuasive
- The victim often becomes immersed in the delusional world the criminals create and responding to the scam can become like an addiction
- The scammers sell information on to other scammers leading on to a snowball effect of scam mail being delivered.

We work closely with Royal Mail and Trading Standards Scotland to crack down on scam mail.



Trading Standards – Case study

This resident lived in an upper flat and was housebound with minimum interaction with the public. He was referred to Trading Standards as his social worker suspected he may have been paying out large sums to different companies. On arrival at his property, the victim denied that he had ever received any mail from anyone he didn't know and had no idea what was going on. From dealing with similar cases it was clear that this gentleman did not have a lot of interaction in his life and the scammers were using grooming techniques to befriend him.

He eventually handed over many letters he had replied to and showed details of cheques he had written amounting to thousands of pounds. This gentleman was in disbelief he: "Wasn't going to finally win his fortune to buy his bungalow down the coast".

He explained that this has been his aim, and he was devastated to realise that these were actually scams.

The following measures were put in place to stop him receiving mail and to also help him with his social isolation.

- Agreed to divert mail to a family member
- Registered for mailing preference service
- Reported issues to Trading Standards and Royal Mail
- Claim made to bank to refund loses.

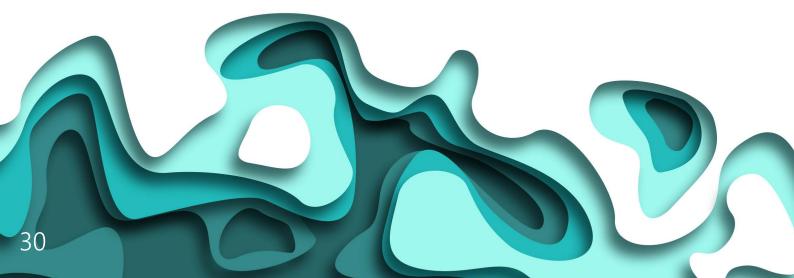
For further information on scam mail contact Trading Standards on: **01463 664570**





Email scam

- Never pay the scam. Paying highlights that you're vulnerable and that you may be targeted again
- Change your password immediately and reset it on any other accounts which use the same one
- Don't reply to the fraudsters
- Update your anti-virus software and operating systems regularly
- · Cover your web cam when not in use.





Blackmail victim

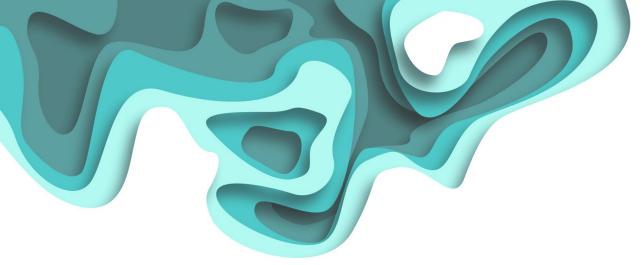
Stay calm - Contact the Police and your local internet service provider as soon as you are made aware of this. The Police will take your case seriously and will deal with it in confidence. You will not be judged for being in this situation.

Don't respond - Don't communicate any further with the criminals. Take screen shots of all the communication that has already taken place and suspend your Facebook account (but don't delete it). This preserves the data and will help the Police to collect evidence. Report the video to Skype and YouTube to ensure it gets blocked and set up an alert in case the video resurfaces.

Don't pay - Demands tend to get higher if you pay and in some cases the videos or pictures may still be posted online. If you have already paid, check to see if the money has been collected. If so, make note of where it was collected from. If it hasn't, then cancel the payment immediately.

Don't delete - Keep all evidence including user names which have been used, the Facebook URL, any links sent to you and any photos/videos that were sent, etc.

Check Skype ID – If you have been using Skype remember that the scammer's Skype name is different to their Skype ID, and it's the ID details that the Police will need. Right click on their profile, select 'View Profile' and then look for the name shown in blue rather than the one above it in black. It'll be next to the word 'Skype' and will have no spaces in it. If this has happened to you or someone you know, you can contact the Police on **101**.



Supported by:











With thanks to:

Age Scotland
OFCOM
NHS Inform

Telephone Preference Service
Neighbourhood Watch Scotland
Office of the Public Guardian (Scotland)
Financial Ombudsman Service
OSCR
Royal Mail

With Special Thanks to:

East Renfrewshire Council for kind use of their original toolkit.