advice direct scotland

2020-21

SCAMS & FINANCIAL HARM TOOLKIT

Introduction

Scams have an impact on Scottish consumers every day, often costing thousands of pounds. Anyone can be the target of a scam, and scammers can be very convincing in their attempts to defraud us of our personal information or money.

Certain demographics are more vulnerable to scams than others. The vulnerable in our society are preferred targets of scammers because of a belief that they will be easier to deceive and the extra difficulty they have in getting help.

In 2015, over **50%** of those over the age of 65 said that they had been the target of a scam. This does not however mean that the vulnerable are the only ones targeted,.

Most of us will be the target of a scammer at some point or another. With information being more readily available, and methods of contact being more accessible, scammers are in a better position than ever to engage with us.

On the flipside, information, technology, and methods of communication can help us too. By being aware of the different methods employed by scammers, we can effectively stop them in their tracks and report scams as they happen.

consumeradvice.scot work with various partners including Trading Standards to help catch scammers in the act and stop them in their tracks.

Our Quick Reporting Tool at scamwatch.scot is available 24 hours a day, 7 days a week.

Always report a scam, they can happen to anyone and reporting prevents other people from being harmed.Help us to do our job in protecting Scottish consumers by reporting suspected scams and suspicious activity to us.

Examples of Scams

Financial Harm:

- Theft
- Fraud
- Exploitation
- Pressure in connection with wills property, inheritance, or financial transactions
- Stopping someone obtaining their money or possessions
- Misusing someone's possessions, property, or benefits
- Being scammed by rogue traders over any method of communication (e.g. telephone and email)

Doorstep Scams and Cold Call Scams:

- 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:

- Impersonation of a bank or other organisation the resident deals with
- selling misrepresented goods and services

Scam Safety Precautions

It is always better to avoid a scam rather than fall foul of a scammer. Being aware of the situations that scammers could potentially exploit for their own gain is important.

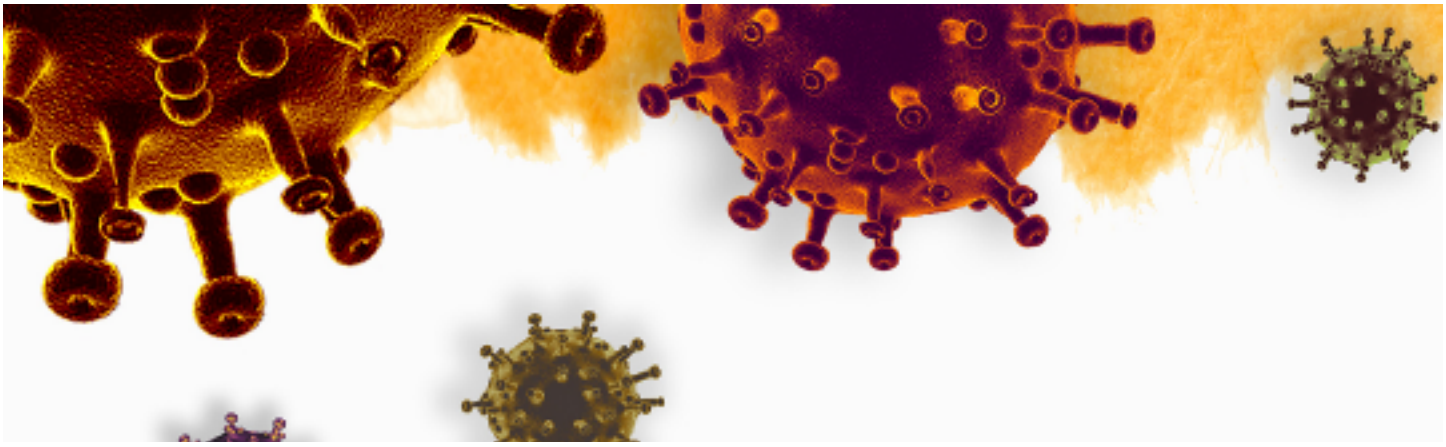
People are particularly vulnerable when they find themselves in certain situations. These include:

- After being diagnosed with dementia or a similar illness.
- After being scammed
- Being socially isolated
- Donating to charities from the door
- Employing cold callers to carry out work
- Financial losses occurring without explanation
- Having recently been bereaved
- Listening to sales chat from cold callers
- Not having access to a list of trusted tradesmen
- Receiving cold calls on the phone or doorstep
- Responding to a seemingly good cause
- Shopping online for the first time or without much experience in doing so
- Using the telephone or dealing with mail without signing up for the Telephone or Mail Preference Service

Scam Prevention Methods

You can take action to reduce the chances of being scammed by:

- Arranging a fire safety visit
- Checking network options with your landline and mobile provider
- Checking that your online activities and accounts are secure
- Considering how any illnesses you have (e.g. dementia) make you vulnerable to scams
- Displaying a “No Cold Calling” sticker on your door
- Getting a call blocking device
- Having access to reputable tradesmen
- Increasing home security with an alarm and a CCTV motion sensor on your doorstep
- Keeping yourself updated with websites that report on scams (e.g.consumeradvice.scot)
- Knowing where to report a scam and who to contact about it
- Learning about the different payment methods with more protections
- Making efforts to reduce your social isolation
- Redirecting your mail where necessary
- Registering for the telephone and mailing preference service
- Researching the risks Power of Attorney if you wish to grant it
- Taking a scam awareness course.
- Taking advice from your bank on how they can protect you from financial harm



Covid-19 Scams

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

Some of the types of Covid-19 scams include:

Testing Kit Scams

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

Test & Protect Scams

In some cases, a message or phone call claiming to be from the NHS Test and Protect Service is sent or made to households claiming they have been in contact with someone who has tested positive for COVID-19 and that they should isolate and take a test. The scammers ask for the citizens home address details so a testing kit can be sent out. Bank details are then requested to "cover the cost of the testing kit".

The public should be aware that the genuine NHS Test and Protect Service will never:

- Ask for bank details, PIN numbers or passwords.
- Ask for any payment or request you purchase any product – including a test.
- Ask you to download any software or ask you to hand over control of your PC, smart phone or tablet.
- Ask that you call any premium rate numbers i.e. 09 or 087 numbers.
- Ask for your social media identities or login details, or those of your contacts.
- Tell you the identity of the person infected.
- Disclose any of your personal or medical information to your contacts.
- Ask you to access any website that does not belong to the Government or NHS.

If you believe you have been the target of a scam, you should contact your bank / service provider as soon as possible if account details have been shared, or money has been transferred / payments made. You should also contact the police to report the situation.

consumeradvice.scot can refer this on to the relevant parties at Trading Standards for investigation.

Scams that exploit those living with dementia

People living with dementia are more vulnerable to scams and other sources of financial harm. They should be protected from scams and safeguards should be put in place to help prevent them being scammed.

Scammers are more likely to target someone vulnerable that will be easier deceive.

Age Scotland have produced a scam prevention guide for those with dementia and those caring for them. It covers protections against financial loss and scams, in addition to practical concerns, such as power of attorney.

The guide can be found here.

Telephone Scams & Nuisance Calls

How to reduce the number of nuisance calls you receive

- Make sure that you do not give your number to organisations that may cold call you.
- Do not give PPI reclaim companies permission to call you. You can report the company to the Information Commissioner's office if they call you without permission.
- You can register with the telephone preference service, who will add your number to a list that companies cannot legally call numbers from.
- Use a call blocking product to prevent nuisance calls. Which? has advice on different products and Ofcom has information on call blocking services that your phone provider has.

What to do if you receive a nuisance call

- Do not give any information, regardless of what they tell you.
- Do not panic. Panic is used by scammers to cause irrational thinking.
- If they claim to be your bank, visit them in person rather than doing anything on the phone.
- If you are in any doubt, hang up. It is always the better option to be cautious.
- Under no circumstances give out any personal or financial information (e.g. bank details).

How to reduce the number of nuisance texts you receive

- If you receive a nuisance text from a company that you have given your number to, reply with the word "STOP" and nothing else.
- If you do not know who is sending the text, do not reply.

How to report a nuisance call or text

You can report nuisance calls and texts to the Information Commissioner's Office.

Silent Calls (line is active but nobody is there)

Silent calls are when you pick up the telephone and there is no noise on the other end.

These calls can also be made accidentally by automatic dialling technology by companies. These automatic diallers can mistake you answering for an answering machine and cuts off the call without playing a message, or hearing anything.

If you are receiving silent calls, you should attempt to identify the caller by dialling '1471'. Silent calls can be reported to Ofcom by calling them on 0300 123 3333, or through their online complaint form atSilent and Abandoned Calls Complaint Monitoring | Ofcom (force.com). If you would rather write to them, you can do this by posting a letter detailing the complaint to:

Ofcom, Riverside House, 2a Southwark Bridge Road, London, SE1 9HA.

You should include information such as:

- The caller's name and telephone number.
- The number of times you have been called by the same number.
- The frequency of the calls.

Ofcom take reports of complaints about silent calls seriously, and may take enforcement action against the company, including imposing fines of up to £2 million.

Missed Call Scams

When you have a missed call on your mobile phone from an unrecognised number, don't call it back until you are sure it's not a scammer.

Scammers can use automatic diallers to contact consumers, with the call lasting very briefly and appearing as a missed call on your mobile.

These numbers vary, either looking like mobile numbers (starting with 070 or 076) or non-geographic numbers (starting with 084, 087, 090, 091, or 118). With all these numbers, you can be charged for the duration any calls you make to them.

When you receive calls from numbers that you do not recognise, take care not to respond to them, as they may charge large amounts for connection and the duration of the call.

If you believe you have been targeted by a scammer, you can report this to your phone provider, by contacting their customer service number, but many now have places on their company websites that you can report these issues.

consumeradvice.scot can also provide information on this, with the police contacted if you have been successfully targeted by a scammer.

Number Spoofing Scams

Number spoofing is when a caller changes their incoming number with the intent of appearing different to the number they are calling from. This can appear as a different number or show as another caller ID (through text messages particularly).

Sometimes, organisations can do this legitimately so that you know who is getting in contact, but sometimes this is the deliberate act of scammers to appear like the legitimate person contacting you.

You should avoid giving any contact information to anyone contacting you directly, and avoid clicking any links in text messages, as this may be the scammer attempting to gather your information fraudulently.

If you are contacted by an organisation claiming to be your bank, or a service provider, they will not mind you asking to call them back. If you choose to do this, ensure that you call the number listed on a previous statement or bill, or the official website for the company / organisation.

If you believe that you have been targeting by a number spoofing scammer and they have gathered information, you should contact the bank / service provider that the scammer claimed to be contacting you from to report this.

You can also report this to the police if the scammer has been successful in gathering information / accessing account, as well as report this to consumeradvice.scot, who can refer this on to Trading Standards on your behalf.

Scam Calls

Scam calls can come in various forms. If you believe that you have been caught out by a scam call, you should report this to the bank / service provider in question as well as the police if you believe they have gathered your sensitive information. They may be able to stop the scammer taking any money or more personal details from your account(s).

You should also report this to consumeradvice.scot who can refer the case on to the relevant Trading Standards department.

Doorstep Scams

Doorstep Scammers arrive at their target's doorstep unannounced and offer unrequested goods and services. Often, they claim to be offering repairs and maintenance of homes and gardens. The prices for these goods and services are heavily inflated and the work/goods are of very low quality.

You should not agree to purchase their goods or services. If they pressure you to accept, do not be afraid to end the conversation and close the door. Call 999 if they scammer tries to intimidate you. If you do not wish to be bothered by salesmen at the doorstep, put up a sticker or sign saying "No Cold Calling" on your door.

Sometimes scammers impersonate Charities on the doorstep to try and extract donation money from their targets. Do not donate to charities on the doorstep unless you are absolutely sure they are no impersonators. If you don't know if it is a real charity, use theScottish Charity Regulatorlist to see if it is officially registered.

How to avoid being scammed by a trader

When using the services of traders, you should not hire them if they come to your door unannounced. Instead you should find one that is reputable and proactively contact them. You can find a trader of repute by using the Trusted Trader Scotland website.

- Check to make sure the trader has an established trading address and landline phone number.
- Do not pay in cash if possible.
- Ensure that your get a receipt.
- Get quotes about the work taking place and the price.
- If the work is not of satisfactory quality, do not pay them until it is rectified.
- Make sure that any guarantees are backed by insurance.
- Put a No Cold Calling notice on your door.
- Under no circumstances should you pay up front.

Postal Scams

Postal scams conducted through the mail can easily deceive targets into paying for low quality or non-existent goods, services and competitions.

Examples of postal scams include:

- Charities and fund raisers.
- Clairvoyance, fortune telling and religious groups.
- Health products.
- Jewellery and similar goods.
- Lotteries, prize draws and other competitions.

Remember that these scams can be very well presented and convincing. Not only should you be on guard for these yourself but be aware of anyone you know that has been targeted.

It is easy for this type of scammer to repeatedly target the same person due to the addictive nature of these mail purchases.

Mail that is fraudulent can be reported to the Royal Mail by writing to Freepost Scam Mail. Alternatively you can email scam.mail@royalmail.com or call 0800 0113 466.

Online Scams (including online purchases)

Huge sums of money are lost annually due to internet-based scams. These either try to pressure a target into giving money or offer goods/services for purchase that are either of low quality or never delivered.

You can keep yourself and your personal information safe when shopping and banking online and surfing the web.

- Do not give bank details to anyone you don't know while online, even if it is a business.
- Do not make payments in advance for a vehicle purchase. Even if they say it is for a deposit or fee.
- Do not open any attachments or links from an unsolicited email address.
- Do not send money to someone claiming to be collecting taxes online. Contact and enquire through the correct government channels in these circumstances.
- If in any doubt, check the details of a website to ensure they are genuine. The padlock on the address bar shows the details of a website.
- If you are asked for money due to an emergency, verify that the emergency is genuine.
- Install anti-virus software on your computer.
- Only buy from well-established sites that you know are genuine.
- Set a password with eight characters that includes at least one number, letter and changed case (e.g. capital letter).
- Under no circumstances should you send money to an individual you have never met in person. This applies regardless of how well you think you know them (e.g. long-distance relationship).
- Use a credit card and avoid sites that don't let you use them. You will not be held liable for fraudulent transactions bought with a credit card and you can claim back funds if a trader you paid goes bust.
- Use unique passwords for every online account and do not share any of them with others.
- You will never be asked to give money in advance for a loan or credit card. Refuse any online business that asks.

Malware Scams

The term 'malware' is an amalgamation of 'malicious' and 'software'. This is a particularly vicious type of cyber-attack that can take various forms. The ultimate motive of the scammer is to obtain control of electronic devices, including PCs, laptops, tablets and other mobile devices.

There are also situations in which the cyber-scammer can use malware to infect a device and then use this to lock the person out of their emails and personal documents, demanding payment to be made in order to remove the virus.

Threats can extend to the information which the hacker has obtained from the victim's device(s), threatening that the individual's web history will be made public (often mentioning the use of adult sites). Even more disturbingly, scammers have threatened to release webcam footage of the victim which they have obtained from the device(s) without the individual's knowledge.

Paying scammer the sums requested rarely solves the problem, and may lead to further instances of extortion; either using the same information to request even more money be paid, or the sale of this information on to other scammers who can make similar attempts.

The most important thing to note when threatened with cyber blackmail is to ensure that no payment is made and immediately inform the police and your internet service provider. These acts are criminal and need to be reported as such.

If you believe you have been the target of a scam, you should contact your bank / service provider in the first instance if account details have been shared, or money has been transferred. You should also contact the police to report the situation.

consumeradvice.scot can refer this on to the relevant parties at Trading Standards for investigation.

Phishing, Vishing, and Smishing (Social Engineering)

- **Phishing** is the use of email and postal methods for a scammer to gather information.
- **Vishing** is the use of the telephone or 'voice' to obtain your personal details.
- **Smishing** is the use of text message or 'SMS' to do the same thing.

All these methods are used by scammers to trick consumers into supplying information that can be used on its own, or paired with additional information to scam, extort or defraud. Stay vigilant – these scammers are very convincing, some even offering links to websites that look like the real deal.

If you believe you have been the target of a scam, you should contact your bank / service provider in the first instance if account details have been shared, or money has been transferred. You should also contact the police to report the situation.

consumeradvice.scot can refer this on to the relevant parties at Trading Standards for investigation.

Romance Scams

Romance scams play on the emotions of the person being scammed. Many of these scammers use flattery and 'love bombing' – i.e. showering a person with compliments and declarations of affection very early on in a conversation to gain trust.

When this trust is built, the scammer uses this and emotional blackmail to gather information or trick the target into giving them money.

People who have been targeted by romance scams can experience embarrassment about being scammed. These scams can often be played out over long periods of time, with the scammer gaining the trust of the consumer being scammed.

If you believe you have been the target of a romance scam, you should contact your bank in the first instance if financial details have been shared, or money has been transferred. You should also contact the police to report the situation.

consumeradvice.scotcan refer this on to the relevant parties at Trading Standards for investigation.

Blackmail

Blackmail scams are an attempt to force payment from a target by threatening them with information that they do not wish certain people, groups or the public to know.

Blackmailers contact the target and show evidence (which may not even be real) of the Target doing something that they wish others would not know.It is important that you remain calm if you are contacted by a blackmailer.

Do not pay the blackmailer under any circumstances. This will not stop them from threatening you and they will ask for more. Do not reply to them.

Instead you should contact the police on 101. Gather all possible evidence to help them resolve the issues. This includes the username and ID of the person that blackmailed you. The police will not pass judgement on you and will keep any information about you confidential.

If this was done online, inform your internet provider. Change any relevant passwords immediately and update any antivirus software. If you were blackmailed over Facebook, suspend but do not delete your account. If the blackmailer used a video to contact you, ask the website to block it.

Banking and Financial Scams

A typical example of banking scams is a fraudster contacting their target and saying fraud has taken place with their bank account. They try to instil panic in the target by saying that their money is not safe. They then offer to transfer it to a save account. This account is actually the fraudster's and is used to access and steal the target's money.

This kind of scam can be avoided if you recognise it. Remember that the bank, police or any other organisation will never ask for any of the following:

- For your 4-digit PIN, password or any other confidential information over the phone.
- To give them goods to hold for safe keeping.
- To purchase anything with your card.
- To send a staff member to your home to collect cash or personal information.
- To transfer money to another account due to fraud or to keep it safe.

If you lost money due to a banking/financial scam and the business refuses to give you a refund, you can escalate the matter to theFinancial Ombudsman Services.

HMRC / Tax Scams

Tax scams try to convince the consumer that they are either owed tax from or owe tax to HMRC. These scams can be very convincing, often displaying the official branding and logos of HMRC.

Tax scammers can also use telephone calls to convince targets to part with their information. Remember that HMRC would never request bank details via email or telephone on their first contact.

If you believe you have been the target of a scam, you should contact your bank / service provider in the first instance if account details have been shared, or money has been transferred. You should also contact the police to report the situation.

consumeradvice.scot can refer this on to the relevant parties at Trading Standards for investigation.

Arranging Power of Attorney and Financial Abuse

Power of attorney is a group of legal arrangements that give someone else the power to manage your affairs. There are three broad categories of power of attorney:

- **General Power of Attorney (GPA)** is only active for a certain period of time and is made in response to a specific situation and responsibility.
- **Continuing Power of Attorney (CPA)** gives a selected person the power to manage both financial and property affairs. While the person whose affairs are managed is still capable of making decisions, they have final say on these matters. It is designed for people who will no longer be able to make decisions in the near future.
- **Welfare Power of Attorney (WPA)** is similar to CPA, except it bestows power over someone's welfare and health. Much like CPA, the person whose affairs are managed has final say as long they can make decisions.

Useful Organisations

Age Scotland

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

Helpline: 0800 124 4222

www.agescotland.org.uk

Advice Direct Scotland

Advice on how to resolve your consumer problems.

Tel: 0808 164 6000

www.consumeradvice.scot

Scottish association for Mental Health

Advice and guidance on dealing with the impact of scams on mental health.

Tel: 0344 800

www.samh.org.uk

The Think Jessica Campaign

Campaign against scam mail.

www.thinkjessica.

OFCOM

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

Tel: 0300 123 3333

www.ofcom.org.uk

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

Telephone Preference Service

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

Tel: 0845 070 0707

www.tpsonline.org.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

Alzheimer Scotland

Leading dementia organisation in Scotland.

Helpline: 0808 808 3000

www.alzscot.org/

Royal Mail

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

Telephone: 0345 611 3413

www.royalmail.com

Office of the Public Guardian

Set up or register a Power of Attorney.

Tel: 0132 467 8398

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

Useful Organisations (Ctnd).

Mail Preference Service

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

Tel: 0207 291 3310

www.mpsonline.org.uk

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

Victim Support Scotland

Provides support to victims and witnesses of crime in Scotland.

Tel: 0345 603 9213

www.victimsupportsco.org.uk

Get Safe Online

Free Expert Advice on online safety

www.getsafeonline.org/

Adult Safety and Protection (ERC)

Worried that someone you know is being harmed or neglected or their property is at risk?

Tel: 0141 800 7850

2021

advice
direct
scotland

Advice Direct Scotland

53 Bothwell Street

Glasgow

G2 6TS

www.advice.scot