CYBER AND FRAUD HUB



A Guide to Avoiding Fraud and Scams for Older People

cyberfraudhub.org

A Guide to Avoiding Fraud and Scams for Older People.

In today's interconnected world, the internet has transformed the way we communicate, learn, make new friends, and access information. While it has brought convenience and opportunities, it has also introduced new challenges, particularly for older individuals. Scammers have increasingly targeted older people, taking advantage of their unfamiliarity with technology or their trusting nature.

This guide aims to empower older adults to navigate the digital landscape safely and securely. It provides insights into common online scams, identifies red flags to watch out for, and outlines steps to take in case of suspected fraud. By understanding the risks and adopting protective measures, individuals can safeguard themselves and reap the rewards of the digital world with confidence.

Five Tips to Avoid Falling Victim to Scams and Fraud

1. Be cautious of unexpected calls, emails, or letters. Scammers often pose as representatives of legitimate organisations, such as banks, HMRC, or utility companies. They may try to pressure you into revealing personal information or taking immediate action. If you're unsure about the legitimacy of a contact, hang up the phone, delete the email, or throw away the letter. Do not click on any links or open any attachments in suspicious emails.

2. Never give out personal information over the phone or email. Legitimate organisations will never ask for your National Insurance number, bank account numbers, or passwords over the phone or email. If someone asks for this information, it's a scam.

3. Be suspicious of any offers that sound too good to be true. If you receive an unsolicited offer that sounds too good to be true, it probably is. Scammers use these tactics to manipulate their victims. If you're unsure about an offer, do your research and get a second opinion.

4. Shred personal documents before throwing them away. Scammers can steal your personal information from discarded documents. To protect your identity, shred all documents that contain sensitive information, such as bank statements, credit card bills, and tax returns.

5. Talk to someone you trust about your finances. If you're concerned about scams or fraud, talk to a trusted friend, family member, or financial adviser. They can help you identify potential scams and support you in making safer financial decisions.



Telephone Scams: Be Aware and Protect Yourself.

Scammers are constantly devising new ways to trick people into giving away their personal information or money. Telephone scams are a common method used to target unsuspecting individuals



How to Spot a Telephone Scam

- **Pushy Sales Tactics:** Be wary of calls from salespeople offering unrealistic discounts or time-limited deals that sound too good to be true.
- **Subscription Renewals:** Legitimate companies will not demand immediate payment for subscription renewals. If you receive a call urging you to pay instantly, it's likely a scam.

- **Computer Access Requests:** Never provide access to your computer to someone you don't know and trust. Scammers may claim your computer is infected or hacked and offer to fix it remotely.
- **Surprise Prizes:** Don't fall for calls claiming you've won a prize. Scammers often use this tactic to gather personal information or trick you into paying for fake prize claims.
- **Personal Information Requests:** Genuine organisations will never ask for sensitive personal information like bank details, passwords, or National Insurance numbers over the phone.

Protect Yourself from Telephone Scams

- **Hang Up:** If you suspect a call is a scam, end the conversation immediately. It's not rude to hang up on suspicious calls.
- **Never Give Out Personal Information:** Do not share personal details, including bank account numbers, passwords, or National Insurance numbers, over the phone unless you are certain you are speaking with a legitimate representative from a trusted organisation.
- **Caller Identification Tools:** Utilise caller identification services or an answering machine to screen your calls. However, be cautious, as scammers can sometimes manipulate caller ID to appear as if they are calling from a known number.
- **Ex-Directory Number:** Consider registering your phone number with the Telephone Preference Service (TPS) to opt out of marketing calls from UK-based companies. Contact the Telephone Preference Service on **0345 070 0707** or visit www.tpsonline.org.uk.
- **Call-Blocking Devices:** Invest in call-blocking devices that allow you to block specific numbers or call types, such as calls from withheld numbers. A lot of these phones can screen numbers coming in without your phone even ringing so you're not even interrupted by these calls.

Additional Precautions

- **Verify Caller Information:** If a caller claims to represent a particular organisation, independently verify their identity and contact information before providing any personal details or making any payments.
- **Beware of Urgency:** Scammers often create a sense of urgency to pressure you into acting impulsively. Don't rush into decisions based on a phone call.
- **Trust Your Instincts:** If something about a call feels off, it probably is. Listen to your instincts and don't hesitate to hang up if you have any doubts.

Report Scams

If you believe you have been the victim of a telephone scam, report it to the Cyber and Fraud Hub on **0808 281 3580** or through our website at cyberfraudhub.org

Further advice is also available from Advice Direct Scotland on **0808 164 6000** or through their website at consumeradvice.scot

If, as a result of a telephone scam, you have lost money then you can report this by calling Police Scotland **on 101**.



Bank Scams.

Bank scams are a growing problem, and older people are often targeted because they are more likely to be trusting and have accumulated more savings. There are a number of things that older people can do to protect themselves against banking scams, including:

Be wary of unsolicited contact. Banks will never call, email, or text you out of the blue asking for your personal or financial information. If you receive a message from someone claiming to be from your bank, but you didn't initiate the contact, don't click on any links or provide any information. Instead, contact your bank directly using the number on the back of your debit or credit card.

Beware of high-pressure sales tactics. Scammers often try to create a sense of urgency or panic in order to pressure you into making a decision without thinking. If someone is trying to pressure you to send money or provide your personal information, don't be afraid to say no and hang up the phone.

Don't give out your personal or financial information to anyone you don't trust. This includes your bank account number, credit card number, National Insurance number, and PIN.

Be careful about what websites you visit and what emails you open. Scammers often create fake websites and emails that look like they are from legitimate companies. If you are unsure whether a website is real, don't enter any personal or financial information.

Keep your computer and mobile devices up to date with the latest security software. This will help to protect you from malware and other threats.

Review your bank statements regularly. This will help you to identify any unauthorised charges. If you see any suspicious charges, contact your bank immediately.

Talk to your family and friends about banking scams. The more people who are aware of the dangers, the less likely they are to fall victim to a scam.

If you think you have been scammed, report it to your bank and the police immediately. You can also report the scam to the Cyber and Fraud Hub on

0808 281 3580

or through our website at

cyberfraudhub.org

Further advice is also available from Advice Direct Scotland on

0808 164 6000

or through their website at

consumeradvice.scot



Here are some additional tips to protect against banking scams:

- Keep a printed copy of important numbers, website addresses and emails for banks, utility suppliers handy, so should you need to, you can contact them quickly to verify any contact you receive.
- Don't give out your personal or financial information over the phone unless you initiated the call and are 100% sure that the organisation is legitimate.
- Be careful about responding to emails or text messages that ask for your personal or financial information.
- Shred any documents that contain your personal or financial information before you throw them away.
- Consider using a credit monitoring service to track your credit report for any unauthorised activity.
- Talk to your bank about security features that can help to protect your account, such as two-factor authentication and fraud alerts.

If you think you've been the victim of banking fraud, do the following:

- Contact your bank or building society immediately.
- If you don't have a number for your bank you can call **159** to get put through directly to your bank.
- Report it to the Cyber and Fraud Hub on **0808 281 3580** or through their website at cyberfraudhub.org
- Further advice is also available from Advice Direct Scotland on **0808 164 6000** or through their website at consumeradvice.scot
- Report the incident to Police Scotland on 101 (non-emergency) or 999 (in an emergency)
- Forward any scam text messages to the National Cyber Security Centre on **7726** (free of charge) and block the number.
- Contact Victim Support Scotland for additional support by calling 0800 160 1985 or visiting their website at - victimsupport.scot

Tips:

- Do not panic.
- Use the phone numbers you have saved, not from any of the messages received.
- Act quickly to increase your chances of getting your money back.
- If you don't feel comfortable contacting the banks directly, ask a trusted family member or close friend to assist you.



WhatsApp Family ar Friends Impersonati

Scammers are increasingly using WhatsApp to impersonate friends and family members to trick people into sending them money. The scam typically starts with a message from a number you don't recognise, claiming to be a friend or family member in need of money who has had to use a different phone from their normal number.



Red flags to look out for:

- Generic greetings like "Hi Gran" or "Hello Dad" to avoid using your name.
- Urgent requests for money.
- Bank account or mobile phone numbers that you don't recognise.
- Account names that don't match the family member who is requesting the money.

nd
on Scams.

1



Figure 1:
An Example of a WhatsApp Scam

2



Figure 2:
Another Example of a WhatsApp Scam

How to protect yourself:

- Be wary of messages from people you don't recognise.
- Don't send money to anyone until you have verified that they are who they say they are.
- Ask the sender a question that only they would know the answer to.
- Never give out your personal or financial information to someone you don't know and trust.

If you think you may have been scammed:

- Contact your bank immediately.
- Report the scam message within WhatsApp. Press and hold on the message bubble, select 'Report' and then follow the instructions.
- Report the incident to Police Scotland by calling 101.

Additional tips:

- If you receive a message from a friend or family member asking for money, try to call them on their usual phone number to verify their identity.
- Be aware that scammers may try to use deception tactics to pressure you into sending them money. They may claim that they are in danger, or that they need money to pay for an unexpected emergency.
- If you are unsure whether a message is legitimate, it is always best to err on the side of caution and not send any money.



Parcel Delivery Scams: How to Spot and Avoid Them.

Parcel delivery scams are a type of scam in which scammers send text messages or emails that look like they're from a legitimate delivery company, such as Royal Mail or DPD. The messages will often say that you have a missed delivery, and that you need to click on a link to reschedule your delivery or pay a fee. If you click on the link, you'll be taken to a fake website that looks like the real website of the delivery company. The website will ask you to enter your personal information, such as your name, address, and credit card details. Once you've entered your information, the scammers will steal it and use it to commit identity theft or fraud.

How to spot a parcel delivery scam:

- The sender's email address or phone number doesn't look quite right. For example, it might have a misspelling or include extra numbers or letters.
- The message is asking you to pay a fee. Legitimate delivery companies will never ask you to pay a fee to reschedule a delivery or to receive a parcel.
- The message has spelling and grammatical errors.
- The message is trying to rush you into action. Scammers want you to act quickly without thinking, so they often create a sense of urgency in their messages.

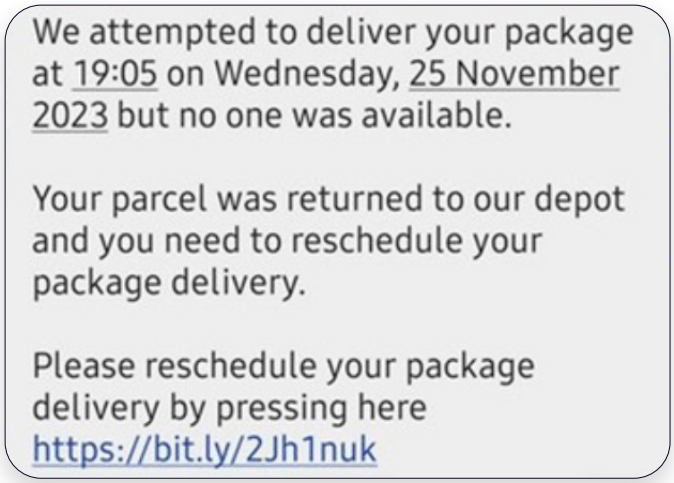


Figure 1:
An Example of a Parcel Delivery Scam

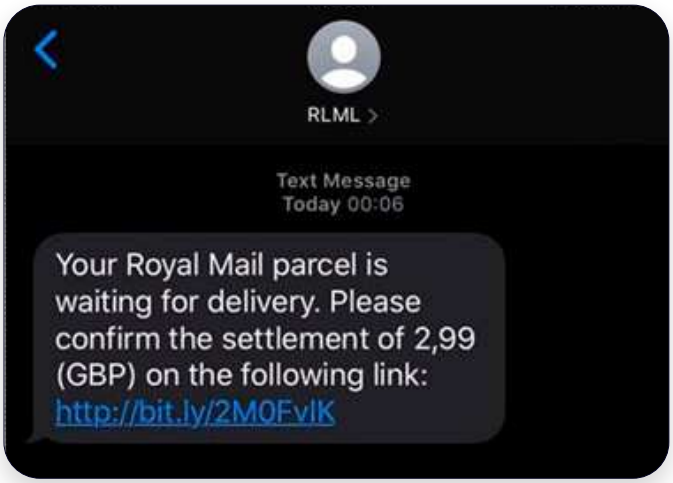


Figure 2:
Another Example of a Parcel Delivery Scam

What to do if you think you've been targeted by a parcel delivery scam:

- Don't click on any links or enter any information.
- Contact the delivery company directly using the contact information on their website.
- Forward any scam text messages to National Cyber Security Centre on **7726** (free of charge) and block the number.
- Forward any scam emails to report@phishing.gov.uk

By following these tips, you can help protect yourself from parcel delivery scams.

Tips to avoid parcel delivery scams:

- Be wary of any unsolicited text messages or emails from delivery companies.
- Never click on links in text messages or emails from delivery companies. Instead, go to the delivery company's website directly by typing the website address into your web browser.
- Never give out your personal information, such as your name, address, or credit card details, to anyone over the phone or online unless you're sure they're legitimate.
- If you're unsure about a message or website, contact the delivery company directly to verify it.

Investment and Pension Scams.

Investment and pension scams can be devastating, and could have a huge impact on your retirement savings. Scammers are clever and can use a variety of tactics to trick people into handing over their money.

How scammers operate

Scammers often use cold calls, emails, or letters to contact potential victims. They may promise high returns on investment, offer "free" pension reviews, or pressure you to make a quick decision.

Red flags to watch out for:

Here are some common red flags that could indicate a pension scam:

- **Unsolicited contact:** If you receive a call, email, or letter out of the blue about your pension, be wary. Legitimate companies will not contact you without your permission.
- **Promises of high returns:** Scammers often promise high returns on investment that are too good to be true. Be sceptical of any investment that guarantees high returns or offers low risk.
- **Pressure to act quickly:** Scammers often try to pressure you into making a quick decision before you have time to consider the risks. Never feel rushed into making a financial decision.
- **Investments in unusual assets:** Scammers may try to sell you investments in unusual assets, such as wine, jewellery, or carbon credits. These investments are usually poor investments, and difficult to sell, if they exist at all, and you could end up losing money.

- **Offers of pension "liberation":** Scammers may offer to help you access your pension savings before you reach retirement age. However, early access to your pension can come with significant tax penalties.

What to do if you think you've been targeted by a scam

If you think you've been targeted by a pension scam, the first thing you should do is stay calm. Do not respond to any further communications from the scammer. Instead, contact the following organisations for help:

- If you have sent money or been defrauded of any funds then you should report this to Police Scotland by calling **101**.
- **The Financial Conduct Authority (FCA):** The FCA is the UK regulator of financial services. You can check whether a company is authorised by the FCA on their website.
- **Pension Wise:** Pension Wise is a free government service that provides impartial guidance on pension matters. You can contact Pension Wise through MoneyHelper. Call the Pension Helpline on **0800 011 3797** or visit the website www.moneyhelper.org.uk
- **An independent financial adviser:** An independent financial adviser can provide you with personalised advice on your pension savings. You can find a list of registered advisers through:
- MoneyHelper – **0800 138 7777** www.moneyhelper.org.uk
- Personal Finance Society – **020 8530 0852** www.thepfs.org

Protecting your pension

You can take steps to protect your pension from scams:

- Be cautious about who you share your pension information with: Do not give your pension details to anyone you do not know and trust.

- Be wary of unsolicited offers: If you receive an unsolicited offer about your pension, be sceptical. Do not respond to the offer without first checking with the FCA or a trusted financial adviser.
- Get independent advice: If you are considering making any changes to your pension arrangements, it is always a good idea to get independent financial advice.

By staying informed and taking precautions, you can help protect your pension from scams.

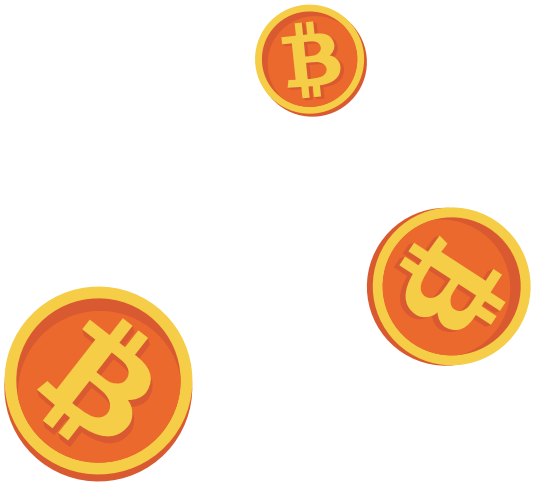


Cryptocurrency Scams.

Cryptocurrency scams are essentially investment scams promoting fake opportunities to buy or trade digital currencies like Bitcoin, Ripple or Ethereum. These complex digital assets confuse many people, making them vulnerable to scammers. Don't invest until you fully understand cryptocurrency and get advice from someone you trust and understand these types of investments fully.

Watch out for "get rich quick" cryptocurrency schemes promising high returns with little risk. They take advantage of the newness and complexity of digital currencies to mislead potential investors. Scammers may use aggressive sales tactics or social media to pressure you to act fast.

You may also be directed to a website that shows huge financial returns relating to small investments. These websites and financial dashboard are completely made up and managed by the scammers.



Beware of these red flags:

- Guaranteed returns - no investment is risk-free.
- Pressure to invest right away.
- Lack of transparency about the company.
- Unsolicited offers via social media, email, texts.
- Requests for remote access to your computer.
- Asking you to share account login details.

Never share sensitive account information. Legitimate investments won't rush or pressure you. Do your research before investing.

The website Chain Abuse (www.chainabuse.com) can help verify cryptocurrency companies and check for ties to scams. Knowledge is your best defence against cryptocurrency fraud. Take time to understand digital currencies before investing.



Identity Theft.

Identity theft is a crime in which someone steals your personal information and uses it to pretend to be you. This can have a devastating impact on your life, as it can lead to financial loss, damage to your credit rating, and even criminal charges.

Here are some signs that you may be a victim of identity theft:

- You receive unfamiliar charges on your credit card or bank statement.
- You receive bills or letters in the name of someone you don't know.
- You are denied credit or a loan, even though you have a good credit history.
- You receive calls or letters from debt collectors about debts you don't owe.
- You find that your National Insurance number has been used to open new accounts in your name.

If you think you may be a victim of identity theft, here are some steps you should take:

- **Contact your bank and credit card companies.** Let them know that you think you may be a victim of identity theft and ask them to close any accounts that have been opened in your name without your permission.
- **Call Police Scotland on 101 to report it.** This will help you with your insurance claims.
- **Place a fraud alert on your credit report.** This will make it more difficult for identity thieves to open new accounts in your name. You can place a fraud alert by contacting a credit referencing agency such as Experian or Equifax.

Here are some tips for preventing identity theft:

- **Protect your personal information.** Don't give out your personal information to anyone you don't know and trust. This includes your National Insurance number, credit card numbers, and bank account numbers.
- **Shred sensitive documents.** Don't throw away sensitive documents, such as bank statements and credit card receipts, in the bin. Instead, shred them.
- **Be careful about what you share online.** Don't share personal information on social media or other websites.
- **Use strong passwords and don't reuse.** Don't use the same password for multiple accounts, one password – one site.
- **Monitor your credit report regularly.** This will help you catch any errors or unauthorised activity.

Identity theft can be a serious problem, but there are steps you can take to protect yourself. By following these tips, you can help to keep your personal information safe.



Safeguarding Yourself from Scams.

Scammers can be cunning and persuasive, but you can take steps to protect yourself. Here are some tips:

Be Wary of Unsolicited Contact

If someone contacts you in an unexpected manner, be suspicious. Scammers often use urgent or threatening language to pressure you into acting impulsively. If something feels off, trust your instincts, and don't respond immediately.

Don't Rush into Decisions

Scammers often try to create a sense of urgency to make you act without thinking. Don't let anyone pressure you into making a decision, especially when it involves money or personal information. Take your time and carefully consider the situation before taking any action.

Seek Advice When Needed

If you're unsure about a situation or feel pressured, don't hesitate to seek advice from someone you trust. Talk to a friend, family member, or a trusted professional. They can help you assess the situation and make an informed decision.

Consider a Power of Attorney

If you have concerns about your ability to manage your finances due to scams or other reasons, consider setting up a Power of Attorney. This would allow a designated person to make financial decisions on your behalf.

Resources for Further Information

For more information on setting up a Power of Attorney, refer to the following resources:

- The Office of the Public Guardian (Scotland)
- Website: www.publicguardian-scotland.gov.uk
- Phone number: **01324 678 300**

By following these tips and staying informed, you can reduce your risk of falling victim to scams. Remember, you're not alone. Many people are targets of scams, and there are resources available to help you protect yourself and your loved ones.



Useful Organisations.

Advice Direct Scotland

Provides all Scottish citizens with practical, relevant and completely free consumer advice and information which makes a difference.

Tel: **0808 800 9060**
www.advicedirect.scot

Age Scotland

Age Scotland is the national charity for people over 50 in Scotland. It is a membership organisation that provides a wide range of services and support to older people and their families.

Tel: **0800 12 44 222**
www.ageuk.org.uk/scotland

Ask Silver

Ask Silver is the easiest way to check if something is a scam. Just send a screenshot of something you want to check via WhatsApp like you would to a family member, and get a reply instantly. It's completely free, has been awarded by the FCA and featured in the Daily Mail and you can sign up at www.ask-silver.com. You can also report scams to the authorities with a single tap, to fight back against fraudsters.

Citizens Advice Scotland

Citizens Advice Scotland (CAS) is a network of independent charities that provide free, confidential, and impartial advice to people in Scotland. CAS has been helping people for over 70 years and is now the largest provider of free legal advice in Scotland.

Tel: **0800 028 1456**
www.citizensadvice.org.uk/scotland

CyberScotland

CyberScotland provides cyber security advice and guidance for Scottish citizens and organisations. CyberScotland aims to improve cyber resilience across Scotland in a coordinated and coherent way.

www.cyberscotland.com

Financial Conduct Authority

The Financial Conduct Authority (FCA) has a number of resources available to help you choose a financial adviser, including a scam warning tool and an online register of authorised firms.

Tel: **0800 111 6768**
www.fca.org.uk

Police Scotland

Contact them in non-emergency situations if you have been the victim of fraud.

Tel: **101** (non-emergencies)
www.scotland.police.uk/contact-us

Telephone Preference Service (TPS)

The Telephone Preference Service (TPS) is a free service that allows individuals to opt out of receiving unsolicited sales and marketing telephone calls.

Tel: **0345 070 0707**
www.tpsonline.org.uk

Trading Standards Scotland

Trading Standards Scotland (TSS) is the national consumer protection agency for Scotland.

Tel: **0808 164 6000**

www.tsscot.co.uk

Victim Support Scotland

Victim Support Scotland (VSS) is a charity that provides free and confidential support to victims of crime in Scotland. VSS helps victims of crime cope with the emotional and practical consequences of crime.

Tel: **0800 160 1985**
www.victimsupportsco.org.uk

Notes

Supporting the Hub

The Cyber and Fraud Hub is supported by:

Arnold Clark

McFadden Associates Limited

twofifths design

CYBER AND FRAUD HUB

0808 281 3580
info@cyberfraudhub.org
cyberfraudhub.org
@CyberFraudHub
cyber-and-fraud-hub

Registered in Scotland. Registered Charity No.SCO53371