The Big Scottish Scam Survey 2022

Overview

The Big Scottish Scam Survey ran from 16 June - 1 August 2022. The aim of the survey was to to find out more about the most commonly experienced scams in Scotland, in advance of a nationwide scams awareness campaign in September 2022.

Highlights

534 people responded to the survey, with responses being received from all **32** Local Authority areas

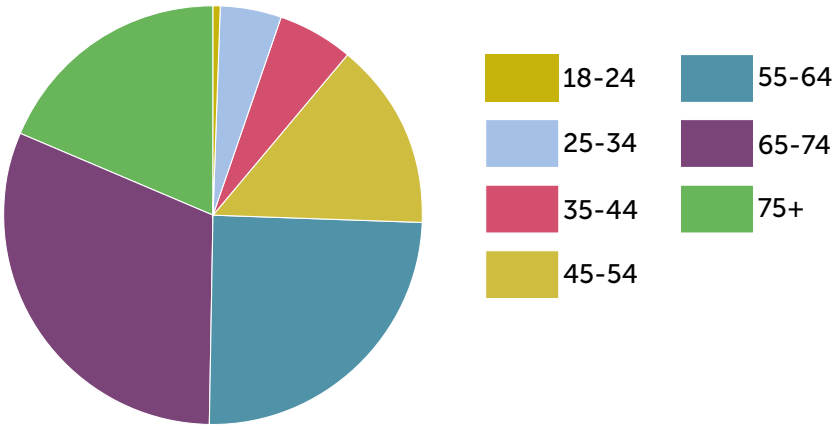
97% of respondents had been targeted by a scam in the past year, either via phone, text message, email, letter or on the doorstep

79% of respondents had avoided a scam after reading or hearing information about it

Demographics

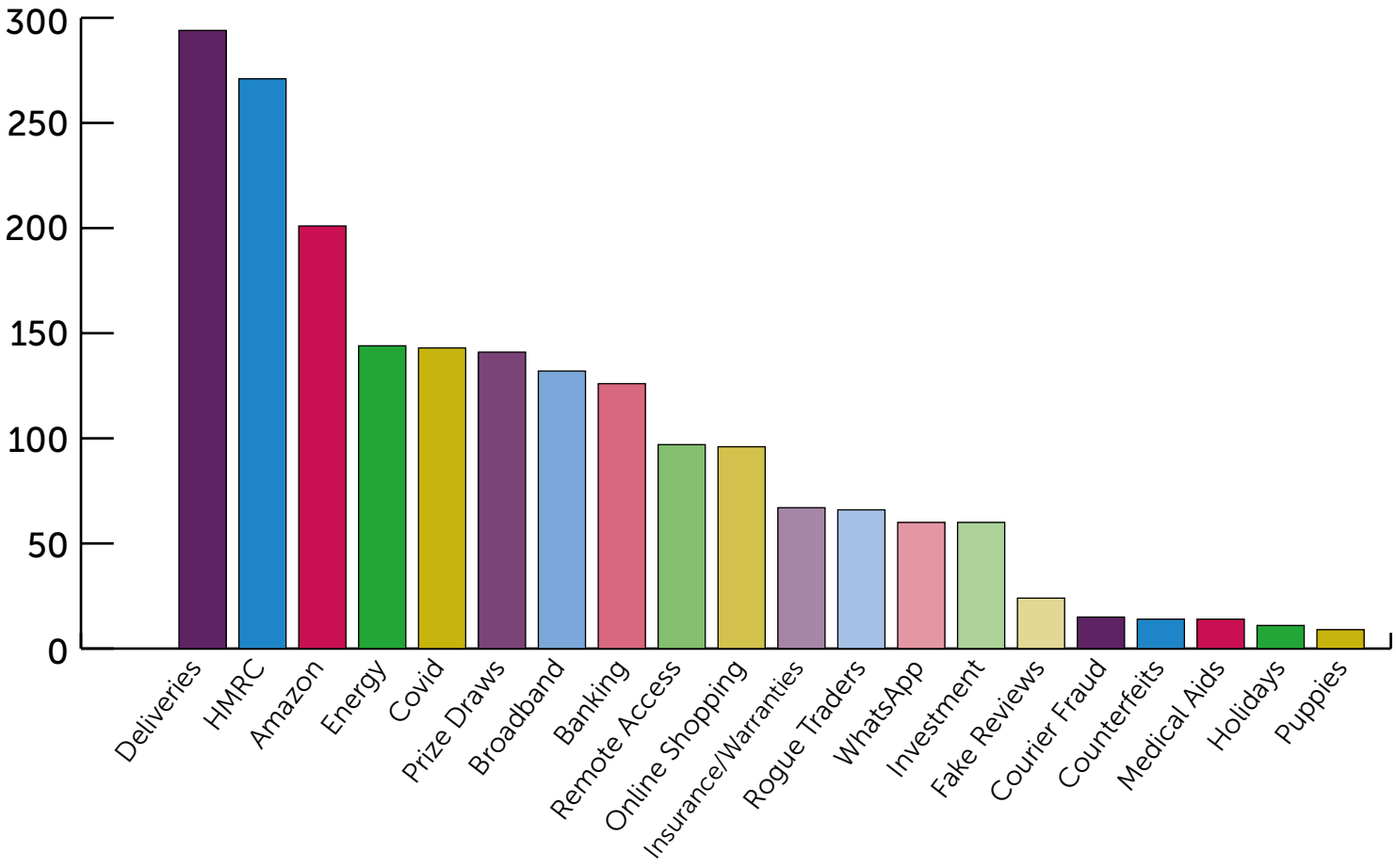
Responses were received from all 32 Local Authority areas in Scotland.

71% of respondants were over 55, with only 7% in the 18-24 age bracket. A detailed overview of the ages of respondents is shown in the chart below:



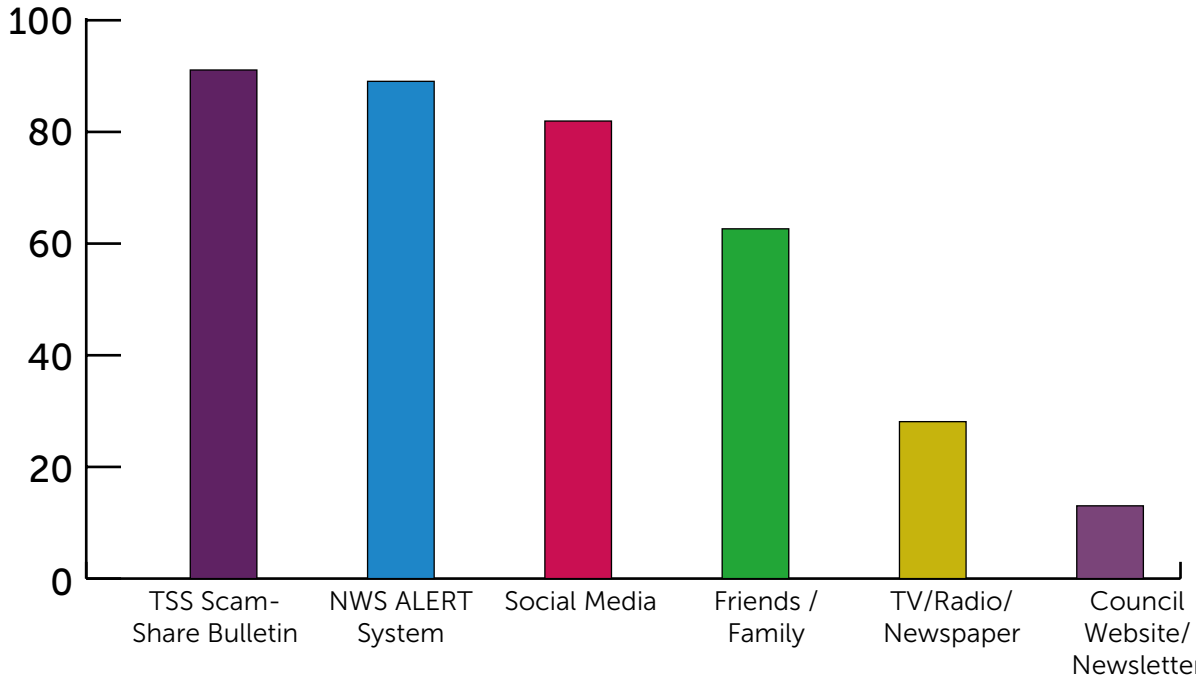
Most Frequently Reported Scams

The following graph shows the number of respondents who had experienced each type of scam. Respondents had the option to tick multiple types of scam.

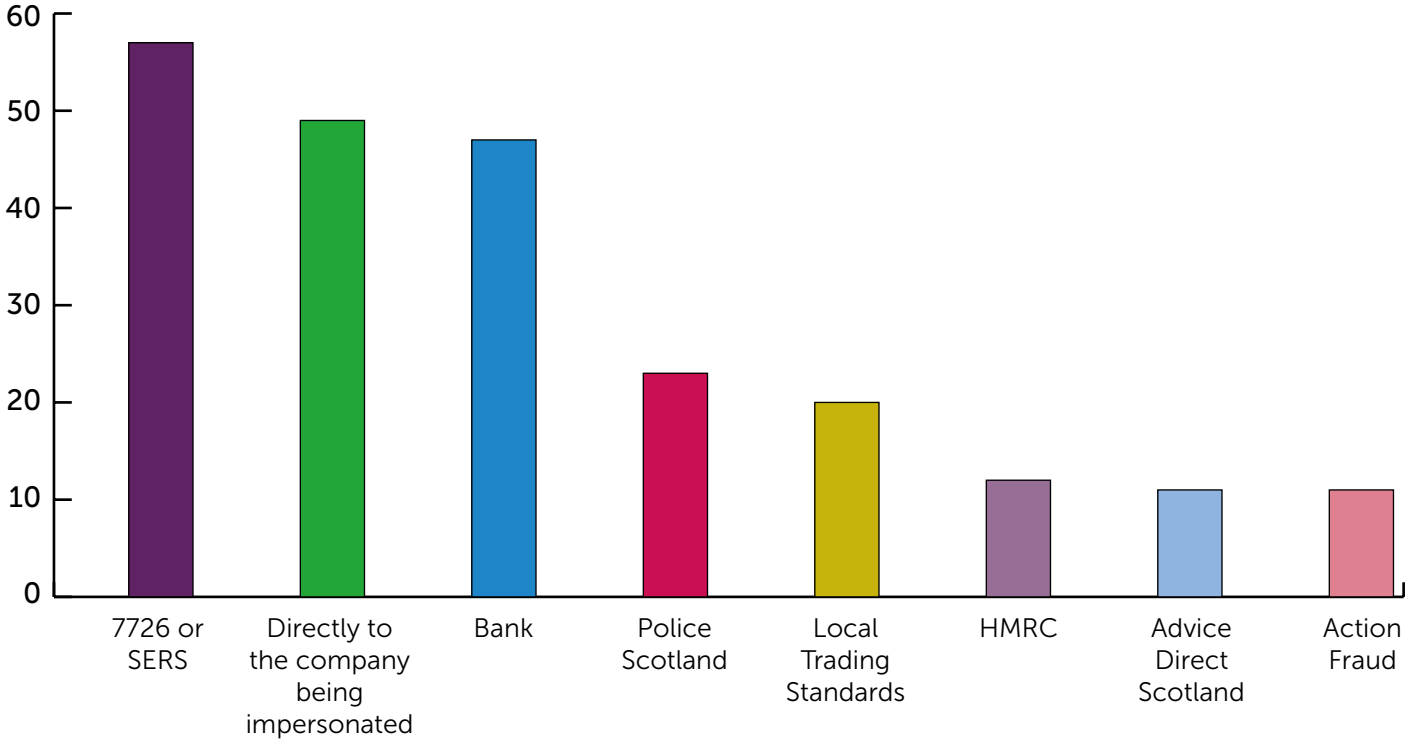


Scam Prevention and Reporting

79% of respondents had avoided a scam after reading or hearing information about it. The graph below provides more detail about where respondents had heard/read about scams.



41% of respondents who experienced a scam had reported it. The following graph shows where scams had been reported.



Loss of Money

For respondents who had lost money to a scam in the past year, the amounts lost ranged from £37 to £25,000.

Scam Examples

The following examples of scams were provided by respondents:

Text pretending to be Royal Mail to say that parcel could not be delivered as no one answered doorbell. Asked for details and £1.20 for redelivery

Cold call from someone posing as BT saying there were problems with my broadband and they needed access to my computer

A man knocked on my front door and offered to clean my driveway, but could only do it that day for a "special price"

Texts advising that as I had been a close contact of someone with Omicron, I should order a test kit via a link

Repeated calls asking us to answer surveys about our property insulation and replacement boilers

Cold call saying there was a visa debit charge of £238 being asked for on my card and if I thought this was fraudulent to press 1. I hung up and checked on my banking app - there was no charge on my card.

Text saying I was entitled to a tax rebate and to click on a link to claim it

Several emails claiming to be from people I know, saying that they are too ill to go shopping, so would I please purchase vouchers as a birthday present for an ill relative

Cold calls from company (with a similar name to our actual insurer) offering discounts on our kitchen appliance insurance

WhatsApp message asking me to help out a relative who had supposedly lost their bank card

Cold call asking if I was over fifty and used a walking stick or frame. They said I could be entitled to a free alert pendant

Automated recording telling me that two payments were due to leave my Amazon account, requesting I press 3 to give permission or phone an 0800 number to speak to someone.

Text saying that my National Insurance number had been compromised

Email saying my PayPal account was about to be closed - I was supposed to click a link to login and stop it happening

A man came to the door and said I could be eligible for government grants for insulating and boiler replacement

Scam Examples

Email teling me that my Sky account was being updated - I was asked for my account details and other info

Text message allegedly from my bank stating a new payee had been successfully added to my account

Cold call saying there had been a possible fraudulent transfer of £600 from my account overseas. I hung up and phoned my bank who assured me no transaction had taken place.

Contractors offering to resurface driveway with tarmac allegedly left over from road resurfacing

Online adverts for 'free' home improvements such as windows or boilers using government grants

Cold call telling me that my National Insurance number had been used to open 12 bank accounts which were being used for criminal purposes. I was told I had to change my NI number and was asked for my bank details so they could 'check which of the accounts was genuine'

Emails saying I have won a competition and asking for bank details to 'claim the prize'

A buyer on Facebook Marketplace said they were using a parcel collection service who would give me cash on collection. They then said I had to pay for 'insurance', but that that I would get my money back from the courier.

Emails saying that my internet security system has expired and asking me to click on a link to pay

Several HMRC texts saying that I either owe money or am due to receive a refund

Email from my energy provider offering me a refund - I had to click on a link and enter my account and bank details

Cold call saying my bank account was at risk and asking me about payees on my account. When they started asking me for log in details I suddenly realised it was a scam

Text saying my Apple Pay account was suspended due to suspicious activity

Email telling me there was a problem with processing my TV Licence direct debit

Cold call supposedly from BT saying that our internet access would be cut off unless we paid an 'outstanding bill'