



From mountain to sea

Doorstep Callers and Scams

Bulletin No. 72

The articles in these bulletins are based on real life complaints made to Aberdeenshire Council's Trading Standards department, unless otherwise stated, to make them as relevant as possible to readers. Names, exact addresses etc. have been withheld to avoid identifying complainants and to comply with GDPR so please feel free to share the contents with friends, family, neighbours or any community groups you are a part of. For details of scams reported in other parts of Scotland, please click [here](#).

Doorstep Callers

One elderly resident of the Garioch area recently reported that he had had three men attend at his front door to advise him that his roof was leaking and that it needed to be repaired. One of these men then used his phone to show the residents some photos of his roof, pointing out the alleged problems.

The resident, recalling that he'd had repairs done to the roof last year and fearing that the same problems had re-emerged, became quite alarmed. Believing that these men were from the same roofing company, he asked what needed to be done. The group's spokesman advised that they could make the repairs but that it would cost almost £1500 and that payment would have to be in cash, so that work could start immediately.

The resident advised the men that his bank was in Aberdeen, so they transported him to the bank in their Transit van where, unfortunately, the bank handed over the cash which the resident then passed onto the men. The group thereafter returned to the resident's home.

On returning there, the men advised that they would need an additional £500 for paint and brushes which the resident felt was excessive and which made him suspicious. He advised them again that he didn't have that amount of money at home and didn't want to go back to the bank that day. The men agreed that they'd come back the next day for the £500. After the men had left the resident called the roofing company which had done the repairs the previous year. This company advised that they never cold called customers, strengthening the resident's suspicions further.

From mountain to sea

Next day, the three men returned but the resident's son answered the door, much to the men's surprise. They asked if the son would like the driveway power-washed or some weeding done, which the son declined. It appears that the son's presence had caught them off-guard. He then asked the men to leave, which they did. They did not come back to undertake any roofing work.

Some points to consider:

- The 'Good Samaritan' approach by passing 'roofers' is a classic tactic of rogue traders. This should be a red flag to any resident that they are probably dealing with a scammer,
- It's unclear what the photos showed but where this sort of tactic is used or actual damage is pointed out and the part of the roof is easily accessible, it is possible that the 'roofer' caused the damage before knocking at the door,
- Rather than asking the cold callers what needed to be done, at that point the resident should have thanked them for their concern, declined their offer then called the original roofing company to discuss them inspecting the roof,
- Requests for payment in cash on the doorstep is another classic scam tactic and is another red flag that the caller is a scammer, or at least dubious,
- Pre-conditions that the work should start immediately should be treated with caution as residents who are approached by doorstep callers for work have a legal 14 day 'cooling off' period during which they can change their minds without penalty. It's wise to use this time, even if it's only a couple of days, for reflection,
- Being taken to the bank by doorstep callers to withdraw a large sum of cash is another classic tactic of scammers, so should be another red flag to residents. However, it is also an opportunity for the resident to ask bank staff for help, particularly if they feel they're being co-erced by the doorstep callers,
- The additional sum of £500 was indeed excessive for paint and brushes unless the men intended to paint the whole house, which had never been discussed,

Remember:

- Never accept offers from doorstep callers like this. The risks are too high that they could be scammers who will take the money and run, or rogue traders who do come back but make such a botch of the job that the resident has to call in real tradesmen to fix their work, incurring even more expense for the householder,

From mountain to sea

- Never allow cold callers access to your roof as they may cause the damage which they then tell you about,
- Never discuss money with cold callers. They will almost always say they can do the work cheaper than anyone else (because they have no intention of coming back to do the work or, if they do, they will use such cheap materials that the work will have to be re-done properly by a real trader). Always change the subject away from money as quickly as you can,
- Politely but firmly thank them for their concern and send them on their way,
- If you think you've had scammers at your door, try to note down details about them and their vehicles, then report the matter to Trading Standards and/or Police Scotland,
- If you think you've been the victim of a scam, please contact your bank as soon as you can to report the matter. You may receive a refund from your bank (though there may be conditions attached to this).

Scams etc.

Banking Scam

One resident of Deeside recently received a call at home from a male claiming to be from his bank. During the call the resident checked the caller ID on the phone and recognised that the number displayed was the correct number for his bank. The caller was polite and sounded credible and already had the resident's name and address.

The caller then asked the resident if he had made a couple of sizable transactions in High Street shops, which the resident advised he hadn't. The caller then asked the resident three security questions, which the resident answered. The caller told the resident that it looked like his account had been hacked and that he should transfer several thousand pounds from his existing accounts into a 'mask' account, via internet banking. The caller provided the resident with the sort code and account number of the mask account and the resident transferred the money, as instructed. A short time later the caller called back and the resident was asked to transfer another several thousand pounds, but this transaction did not go through.

At this point the resident became suspicious and hung up on the caller. He then called his bank and reported the matter, only to be told that it appeared that he had been scammed by the caller. Enquiries with the bank are ongoing.

In truth, this is the classic safe account scam with a couple of twists. These twists are that the caller asked the resident the security questions and got the



From mountain to sea

caller to make the transaction rather than do it himself. It's likely that the resident could have provided any answer to the security questions and the caller would have accepted them, as they were simply a red herring to what was really going on.

The second transaction was actually stopped by the bank's computers which had picked up that something was amiss.

Some points to consider:

- This is a classic telephone scam. If you receive such a call – hang up immediately. Do not listen to any more of the caller's lies,
- The two transactions mentioned by the caller never happened. Their purpose was to alarm the resident to get him to panic and act rashly. This is a typical tactic of a scammer and not how legitimate banks operate,
- As mentioned before, never trust Caller ID on its own as scammers have access to computers which can spoof real numbers (spoof – show a false number on the display while concealing the caller's true number). Look for other proof that the caller is who they say they are and if you're not happy, hang up,
- The caller asking the security questions was a red herring to gain credibility and convince the resident that it was actually his bank calling. It's unlikely that the caller had the correct answers with him,
- The bank account details which the caller provided to the resident were most likely the scammer's own account,
- If you receive such a call, after you've hung up – stop. Do nothing until you have carefully considered what has just happened. Ask someone else what their opinion of events is and if they think it might have been a scam. Do not act rashly, take time to think things through,
- If you think it was possibly a scam call, call your bank to report the matter but when you go back to the phone and lift the receiver, listen for a dial tone so you can be sure that the scammer is not still on the line. Otherwise, use a different phone to call your bank,
- If you think you've been the victim of a scam, remember to also report the matter to Police Scotland and/or Trading Standards. Contact details are at the end of this bulletin,

BUT, most of all, NEVER transfer money out of your bank account as a result of any cold call.

Misc.



From mountain to sea

A recent survey of Trading Standards officers across the UK by the Chartered Trading Standards Institute (CTSI) found that Facebook Marketplace is the most complained about online platform. Some of the grounds for complaint included being slow to act against problem traders and enabling counterfeit goods and potentially harmful products to re-appear on its platform after already being taken down.

That said, other online platforms were also found to be problematic.

The full article can be read by clicking [here](#).

Conclusion

Please note that the advice given in these bulletins has been deliberately kept simple, so that if you are faced with such a scenario where fear, alarm and panic are tools often used deliberately by scammers, you will know what to do at that time.

If you have been the victim of a Bogus Caller or other form of scam, please report the matter to Consumer Advice Scotland so that Trading Standards can maintain a detailed picture about scammers operating in the Shire. This would be a great help to us to tackle this sort of crime.

If you have any information to share about the unlawful sale of tobacco or disposable vapes, please use the Contact Info below to pass that information to Trading Standards. If you would prefer, you can report the information anonymously to Crimestoppers on 0800 555 111.

Contact Info

For non-urgent Trading Standards enquiries in Aberdeenshire, please contact Consumer Advice Scotland at <https://www.consumeradvice.scot/> or on 0808 164 6000. For urgent Trading Standards matters, contact Aberdeenshire Council's Trading Standards at 01467 537222.

Aberdeen City Council's Trading Standards department can be contacted by calling 0300 0200 292 or e-mailing tradingstandards@aberdeencity.gov.uk

Contact Police Scotland on 999 if you need urgent Police assistance or 101 for non-urgent matters.



From mountain to sea

For more information about scams please visit Friends Against Scams at <https://www.friendsagainstscams.org.uk/> or Take Five at <https://takefive-stopfraud.org.uk/>

Please direct any media queries to news@aberdeenshire.gov.uk or 01467 538222 during office hours.

All previous Trading Standards bulletins can be found at:
<http://publications.aberdeenshire.gov.uk/dataset/trading-standards-crime-and-scams-bulletin>