Aberdeenshire COUNCIL

From mountain to sea

# Trading Standards Scams Bulletin No. 121

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 on the Trading Standards Scotland Bulletin page.

## Bogus Callers and Rogue Traders

One elderly resident in the Banff and Buchan area recently had a cold caller at his door who he recognised from last year as being a rogue trader who had done some work and, after the rogue trader had left, the resident had come to the conclusion that the work had been overpriced and very shoddily done. So far, so normal.

However, this resident had formulated the plan that he could engage the rogue trader once again and then refuse to pay for this year's work to compensate for last year's efforts, so had asked him to come back at a later date. While the rogue was at the door, the resident openly took a photograph of one of his associates who was standing nearby. He also covertly took a note of registration number of the rogue's vehicle.

The resident then contacted Trading Standards to seek advice about his plan. He also advised that he had been targetted by other rogue traders since being scammed last year. While it is understandable that the resident was still aggrieved about last year's events, the possible repercussions of his plan were explained to him and he was strongly advised not to go ahead with it.

Some points to note:

- Needless to say, this is a risky strategy as once the rogue trader has ascertained the resident's true intentions, things could turn very nasty,
- The resident's safety and welfare is far more important than the money he lost last year. It is this position which underscores our advice when dealing with any cold caller at the door – be polite but firm; "thanks but no

thanks"; don't get drawn into discussing money or get into an argument; then close and lock the door,
- Please see Scams Bulletin 104 here for more details of how to deal with cold callers, but in a nutshell it's "thanks but no thanks" to all cold callers,
- It is highly likely that this rogue trader came back this year to have another go due to him successfully scamming the resident last year,
- It is also highly likely that the other cold callers came to the resident's door as his details had been shared or sold by the rogue trader. This selling of information is common practice amongst cold callers who figure that if someone falls for one scam they may well fall for another,
- The likelihood of having cold callers come to the door can be reduced by having 'No Cold Callers' notices and stickers on the garden gate and by the front door,
- Openly taking a photograph of a cold caller at the door is a risky matter, and is to be discouraged, as it may cause a hostile reaction. Any photographs taken should be done discreetly, then shared with the Police or Trading Standards. Posting these photos on social media to identify the person in the photo would be a breach of the Data Protection Act 2018 and thereby a criminal offence, so should be avoided,
- Noting the registration number, make and model and any business info on the side of a cold caller's vehicle, if done discreetly, is fine and this information should then be passed to Trading Standards or the Police,
- It is understandable that the resident would want to get some recompense for his money from last year, but this was not the way to go about it. Far safer to report matters to Trading Standards for us to pursue.

## Scams etc.

Remote Access scam

For the first time in a long time Trading Standards have had a report of a vintage scam, the remote access scam.

An elderly resident in the Kincardineshire area recently reported that he had received a phone call from a man claiming to work for Microsoft. This man claimed to be calling as he was aware that the resident's computer was not working properly. He also claimed that for a small charge he could fix the problem and have the computer running smoothly again in no time.

Unfortunately, the resident agreed to the caller's request and followed his instructions to allow remote access to the computer. The caller then advised the resident that the charge for the service would have to be paid up-front, before any 'repairs' were done. As he was already committed, the resident provided the

caller with the 16 digit number on the front of his debit card. When it came to providing the 3 digit security number on the back of the card, the resident then had second thoughts and refused to proceed any further. He then put the phone down.

Later he reported the matter to Trading Standards, although details of the incident are limited. However, what is clear is that this is a remote access scam, which we had hoped we had seen the last of.

Some points to consider:

- Microsoft was never involved in this scam in any way. Its name was simply misused by the scammer to give the scam some credibility,
- Tech companies like Microsoft do not call people up to advise them that there are problems on their devices,
- This is a scam which has been almost unheard of for many years as it had become so well known to the general public and had all but lost its ability to deceive,
- It is unclear where the scammer would have obtained the resident's phone number and personal details,
- Thankfully, the resident held no banking details on his computer, which is often what these types of scammers are looking for, so that they can try to steal from a victim's bank account,
- This type of scam often begins with worrying looking pop-up messages appearing on the device's screen,
- This type of scam also involves the resident following a number of instructions from the caller, sometimes to download apps or programs onto the device, which will then result in the caller being able to access the resident's device from almost anywhere on the internet,
- Never allow a cold caller access to any of your devices, no matter who they say they are. As with cold callers at the front door, it's "thanks, but no thanks",
- If you have any concerns about any such call, simply hang up. Don't waste time with the caller or get into a conversation; just hang up,
- Never give your personal details over the phone to a cold caller, let them confirm who they want to speak to first. Also, NEVER give over any financial information to any cold caller on the phone…ever,
- If your device is not working properly, then consider contacting well-known names like Currys, PC World, the Apple Store or independent computer experts who you have had recommended by friends or family and who have had work well done by those experts to their satisfaction,
- If you think that someone has gained remote access to your desktop computer, the quickest way to deal with it is to simply shut down the

electricity supply to the computer. This will cut the connection to the internet immediately and shut out the scammer,
- For other devices, shut the device down completely rather than just switching it off, then seek help,
- If you think your bank details or bank account have been compromised, please contact your bank immediately and report the matter to them. Consider using the Stop Scams short code of 159 to do this,
- Also, consider reporting the matter to Police Scotland and please report the matter to your local Trading Standards office.

Further information about computer crime can be accessed on the Police Scotland website here.

## Misc.

#NoBlameNoShame Campaign 2025
The No Blame, No Shame 2025 campaign commenced on Monday 15th September and, as with previous years, the focus of this campaign is to avoid victim blaming and shaming. It is a simple fact that everyone can be susceptible to scams, no matter who they are. A major factor in almost every scam involves manipulation or coercive control.

This susceptibility could be down to pure circumstance; that someone, anyone, is just having a bad day and that happens to be the day when a scammer calls. It may also be down to other factors such as health issues, disability, mental health issues, bereavement or unfamiliarity with technology. There are many other possible factors besides these.

One aspect of falling victim of a scam, which is rarely mentioned, is the impact it can have on people (of any age) such as anxiety, depression, embarrassment and shame. Ultimately, the point of these campaigns is that victims should not be blamed for falling for a scam (there is only person to blame and that is the scammer) and that there should be no shame attached to falling for a scam as many scammers are clever, manipulative and well resourced individuals who have made a multi-billion pound, global, criminal industry out of scams.

Further information about the #NoBlameNoShame Campaign 2025 can be found on the Friends Against Scams website here.

## Conclusion

Aberdeenshire COUNCIL

From mountain to sea

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://consumeradvice.scot/contact/ or call them on 0808 164 6000.

For urgent Trading Standards matters or doorstep crime matters, contact Aberdeenshire Council's Trading Standards at 01467 537222 or via trading.standards@aberdeenshire.gov.uk

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.

For more information about scams please visit the Friends Against Scams website or Take Five at their website.

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

All previous Trading Standards bulletins can be found on the Aberdeenshire Council website on the Trading Standards Scams Bulletin page.