Aberdeenshire COUNCIL

From mountain to sea

Trading Standards Scams Bulletin No. 146

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 resident in the east Marr area recently reported to that he had had a male cold caller at his door who had caused him sufficient concern that he felt the need to report the incident.

This cold caller had attended the resident's home address with claims that he had spare tar and road chippings left over from a nearby job and the caller wondered if the resident would like some ground repairs done at his property using these materials. The resident could see no signs of road tar or chippings, so rightly said that he wasn't interested. The cold caller made to leave but when doing so he looked past the resident into the house, as if taking stock of what was inside.

The cold caller then got back into his vehicle, but before driving off he again seemed to show undue interest in his surroundings, looking around with great interest at the resident's property. The resident felt this behaviour to be very suspicious.

Some points to note:

- Claims by cold callers of having spare road tar and other materials left over from a nearby job are common tactics of rogue traders and scammers,
- This cold caller's obvious undue interest in the inside of the resident's home and garden may have been an indication that he was scouting the location for a return visit,

- In other circumstances, behaviour similar to this has caused people to fear that a cold caller was actually looking to see if there were things worth stealing,
- The cold caller was described as being male, white, around 50 years of age, balding and overweight,
- His vehicle was described as being a small white van with a 'Highway Maintenance' sticker on the rear,
- This incident again underscores why you should not entertain any cold caller at the door as you really do not know their real intentions,
- Instead, remain firm but polite, say "Thanks but no thanks", don't get drawn into a debate about the matter; simply step back then close and lock the door. If you think it's justified and can do so discreetly, keep an eye on the cold caller as they leave,
- As with this resident, if you are sufficiently concerned by the cold caller's behaviour, please report the matter to your local Trading Standards office or to Police Scotland.

E-mail scam

One resident in the Garioch area recently received an e-mail from a former college whom he hadn't seen for a while. The e-mail was from a private e-mail address, one which incorporated the former colleague's name in the e-mail address and which had her name appended to the bottom of the message. It asked the resident if he had time to chat over e-mail. At that time he had no concerns about the e-mail, so replied to say that he did have a little time to chat.

A short time later the resident received a response from the sender. This e-mail asked the resident for help. The sender stated that she needed to get a gift card for a friend who was dealing with cancer and whose birthday it was that day. The e-mail went on to say that the sender was out of town and had tried to get a voucher online but without success. Finally, the e-mail asked if the resident could buy an Amazon gift voucher on the sender's behalf, send it on to her and she would reimburse the resident. No value was specified at that time.

At this point, as the resident is a reader of this Bulletin and had read of similar events before, he became a little suspicious and ended all e-mail contact via that particular e-mail address. Instead he called the sender on the phone and she confirmed that she had not e-mailed the resident recently and certainly not about gift vouchers. The truth of the matter was that it was indeed a scam and the narrative pitched was a complete fabrication. The resident then reported the matter to Trading Standards.

Some points to note:

- Amazon, of course, had no active part to play in this scam. It was simply the preferred option of this scammer in whose gift vouchers they would like to spend,
- We have seen similar scams before, where the conversation is directed from the start to take place over e-mail as, if the parties were to use a phone, the resident would realise immediately that the other person was not his former colleague but a scammer,
- The initial e-mail was quite short. No doubt this was to save the sender time, to see if they would get a reply or not. If not, they would probably have moved on to another e-mail address very quickly,
- Once a reply had been received, the scam was pitched. As can be seen, the scam rested on the lie of a friend dealing with cancer, showing how low some scammers will sink, in playing with peoples feelings about such a horrible disease. Of course, the story the scammer pitched was just that, a story, but one they intended to benefit from,
- The crux of this scam is that if the resident had bought the gift voucher the scammer would have asked for the details like the serial number to redeem the voucher for 'the friend' (in reality themselves) and the resident would never have received any reimbursement,
- Our enquiries suggest that the scammer was able to attempt this scam because the e-mail account had had its password hacked and changed by the scammer (thereby locking out the real account holder) and the scammer had then started sending out e-mails to people listed in the Contacts section of the account,
- To prevent this, strong passwords should be at least 12 characters long with at least 1 capital letter, 1 lower case letter, 1 number and 1 special character like a question mark, exclamation mark or similar,
- Many e-mail providers ask customers for details of a rescue e-mail address so that if the customer is locked out of their e-mail address and need to change the password, the security link to do this is sent to the rescue e-mail address, not the hacked one. These two e-mail addresses should never have the same password or the hacker may be able to access both of them,
- As an alternative to a strong password, using 3 completely random words is a good way to keep accounts secure as the hacker will find it almost impossible to guess these words. Conversely, the word 'password', pets' names, children's names, birthdays etc. should also never be used as they may be easy for a hacker to guess,
- If you receive any similar e-mails, no matter who they purport to be from, but especially if they try to pull on a recipient's heartstrings because of someone dealing with cancer and the sender has a sore throat or laryngitis, be very cautious that it may be a scam. If in any doubt, end all contact by e-mail. Use a different method to contact the real sender to query the matter with them,

- If you think you have been the victim of an e-mail scam like this please contact Trading Standards for advice on how to deal with the situation.

Misc.

Face the Fakes campaign



On Friday 30th October 2026, the Intellectual Property Office (IPO) launched the 'Face the Fakes' campaign, highlighting the dangers posed by counterfeit cosmetics and health products.

This comes as testing by the IPO and Trading Standards found 4 in 10 seized counterfeit cosmetics contained potentially harmful substances, including mercury, excessive lead, methanol and nicotine.

The campaign is supported by new data from the IPO, Trading Standards and beauty industry experts on the issue. Testing identified one skincare product containing 13,200 parts per million of mercury, excessive lead in make-up and a counterfeit fragrance made up of around 80% methanol (sometimes known as wood spirit, which is highly flammable).

The campaign also aims to highlight safety advice from an expert toxicologist, and backing from the beauty industry including the British Beauty Council and

the Cosmetic, Toiletry and Perfumery Association. The IPO has also worked with Giorgia Aloi, who launched safeglam.co.uk to raise awareness of the harms of fake cosmetics after her mum experienced a rash and scarring after unknowingly using fake make up.

The campaign's main aim is to show consumers and businesses that counterfeit beauty products are a growing problem, with cosmetics, skincare and perfumes now among Trading Standards' ten most commonly investigated fakes, and that buying from untrusted sellers can put health and safety at real risk, particularly as counterfeit beauty buying rises sharply among younger consumers. The campaign highlights key advice for spotting and avoiding fakes when shopping online.

Further information about the campaign can be found on the British Beauty Council's website here, on the BBC News website here and on the ITV News website 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://consumeradvice.scot/contact/ or call them on 0808 164 6000.

Aberdeenshire COUNCIL

From mountain to sea

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.

Follow us on Facebook at https://www.facebook.com/TradingStandardsAberdeenshire