Aberdeenshire COUNCIL

From mountain to sea

Trading Standards Scams Bulletin No. 147

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 Buchan area recently reported that he had had two male cold callers at his door purporting to be from Kingdom Coatings, a Stirling based company. These callers claimed that the resident's roof looked as if it had a substantial build-up of moss on it which needed attended to urgently and that the roof would need a special coating on it afterwards.

The resident was already aware of a relative who had been pestered repeatedly with similar cold callers, so politely declined the offer. The two males became very insistent, refusing to take a polite no for an answer and they kept badgering the resident to allow them to work on his roof.

Despite feeling somewhat intimidated, the resident remained polite but firm and stuck to his guns. Seeing that the resident would not be swayed, the pair became quite insolent and cheeky towards him but eventually they left. Trading Standards were subsequently notified.

Some points to note:

- Trading Standards position on cold callers at the door is unchanged. You don't know who they really are or what their true motive is, so the safest response is a polite "thanks but no thanks",
- Passers-by who claim to be roofers of one sort or another and who also claim to have noticed a serious issue with your roof which just has to be attended to immediately is a classic tactic of the rogue trader,
- If caught in a similar situation, remain polite but firm and stick to your guns, even in a challenging situation like this one,

- It is unclear if these cold callers' claims had any merit in them at all. Any build up of moss on the roof may have not been grounds for any concerns nor the need for any additional coating either,
- To avoid having callers like this come to your door it may be worth having a genuine roofer inspect your roof on a regular basis, such as annually, and for them to take care of any developing issues. Please be aware though that good roofers are often booked months ahead so prepare early for this eventuality,
- To identify genuine roofers, speak to friends, family, neighbours etc, to see if they have had work done, who did it and were they happy with the outcome,
- Please NEVER go looking for tradesmen on social media. Social media is the root of many, many complaints which Trading Standards receive, so please be very cautious whenever using it,
- Please also be cautious when using certain trade websites as rogue traders frequent these spaces, pretending to be genuine tradesmen, but actually they're looking for their next victim. Please consider the Aberdeenshire Trusted Trader website instead or the City or Moray equivalents,
- Remember, if you have a cold caller come to your door, try to see discreetly who it is (through a side window, door viewer, video doorbell etc.) before you answer the door. If you don't like the look of them, you're not obliged to answer the door,
- Remember too, to report incidents like this to your local Trading Standards office so that we can alert and advise other people.

Scams etc.

Investment scam

One Buchan resident recently advised Trading Standards that he had seen an advert on Facebook by an American company based in Chicago which claimed that by using AI that it could turn modest investments into large profits for investors.

Intrigued by this, the resident clicked on the advert and was taken to an external website where he was asked to input his personal details and to make an initial investment of £200, which he did. As a result, the resident was allocated his own investment advisor. Over the next few weeks, he was advised regularly on how his investment was increasing in value.

Two weeks later, the resident was contacted by his investment advisor who told him that if wanted to make real gains he should start investing in gold. The

resident agreed to this and shortly afterwards the investment advisor's company started making large deposits into the resident's bank account, totalling tens of thousands of pounds. The resident was then advised to start buying up gold ingots, so started to do so via a local business, to the tune of £25,000.

The resident was later contacted again by the investment advisor. This time he suggested the resident re-invest the gold, to make even bigger profits. The advisor also stated that to start this process he would have a private courier attend at the resident's home address to uplift the gold ingots and take them away for investment.

It was just after this that the resident learned that someone had used his personal details to take out loans in his name with 3 separate banks to the value of £50,000, all without his knowledge or consent and which were then deposited in his bank account to fund the gold purchases. At no time was he told by the investment company where this money came from.

On learning this and realising that he had been scammed, the resident contacted Police Scotland, his bank and, later, Trading Standards, to seek help in dealing with the situation. That help is still ongoing.

Some points to note:

- Facebook took no active part in this matter; its platform was simply the one chosen by the scammers to snare their victim,
- As we have said many times before, Facebook is often a hunting ground for scammers looking for their next victim,
- The crux of this scam is that once the gold had been uplifted by the courier, the resident would never have seen it again and he would have been left with the tens of thousands of pounds of debt in loans to pay off while the scammers kept the gold and made themselves £25,000 better off. This example also shows just how callous scammers are to the situation they leave their victims in once the scam is complete,
- There is also a chance the scammers will use the resident's personal and banking details to take out further loans or other credit agreements with other lenders which he may not find out about for some time and which he will also be left to sort out, no doubt causing him further substantial stress and anxiety,
- This incident perhaps underscores the need to diligently keep personal and banking details confidential from those who do not need to legitimately know them - and the dangers which await in providing them to the wrong sort of person,
- Please be very wary of clicking on adverts on Facebook or any other social medium. If you see an advert for something which interests you,

open a fresh web page and make an open source internet search on the company concerned to find out more about it; i.e. is it reputable or not? Has it been linked to scams in the past? Remember to include checks on sites like Trustpilot or Tripadvisor,

- If you think you may have been the victim of a bank-related scam, please report the matter to your bank as soon as you can. Use the Stop Scams short code of 159 on your phone to expedite matters,
- In this instance, due to the sums involved and the clear criminality involved, this is also a Police matter,
- In these circumstances, it may also be useful for someone who has inadvertently given their personal and banking details to scammers to create an account with the 3 large credit scoring companies; Experian, Equifax and TransUnion and make regular checks on their accounts there, to see if the scammers have tried to take out any other credit agreements. If so, contact the company concerned and tell them what has happened,
- As always, please also report matters like this to Trading Standards, so that we can offer advice and warn others about these scams,
- Finally, please remember, if an investment scheme appears too good to be true, it very probably is.

Misc.

I am obliged to Alan Parker of SHMU FM for the next article which is about a matter which could affect anyone who browses online.

ClickFix Scam

The Guardian newspaper recently ran an article which highlighted a growing scam. This involves a process many of us barely notice when using our computers and devices online.

When trying to access certain websites, we may be asked to verify that we are not a malicious bot trying to access the site by clicking on pictures of buses or bicycles in a grid of photos, or we may be asked to input a grainy series of numbers or letters into another box on the screen. This is a legitimate way of confirming that the agent trying to access the website is in fact human. This is the Captcha system. So far, so normal.

In a scam called ClickFix, instead of the Captcha request being made, device users see a different message asking the user to complete a number of steps involving ticking a box on a pop-up box to verify you are human (which actually permits a malicious infection to be downloaded silently onto your device), then

pressing the Windows button and the 'R' button simultaneously (this normally opens the Run dialog box in the bottom left corner of the screen), then the Ctrl (Control) and 'V' buttons simultaneously (this is the Paste function for text) and finally pressing the Enter button on your keyboard. This then enables the downloaded malicious programme to infect your device.

These programmes can be designed to steal your passwords and send them to the hacker, to lock your device until you pay a sum of money (ransomware) or Trojans to allow the hacker remote access to the device.

Some points to note:

- Genuine Captchas will not ask you to press the Windows and R button or to paste any text,
- If you are asked to do so, be very suspicious. Instead, close the webpage immediately,
- If you have already started following the instructions before you become suspicious, disconnect from the internet and shut the device down completely (don't just turn it off),
- The first thing you should do once you re-start the device is to run the anti-virus and spyware programmes to capture any malware which may have been downloaded before you shut the device down,
- Remember, preparation is often the key to dealing with scams, so always ensure your device's security suite is up to date by have the update settings for the suite set to automatic or recommended, so that the suite will update without you having to do anything and possibly without you even knowing it's happening,
- If you think you've been the victim of such a scam, please report the matter to Police Scotland or Trading Standards for advice.

The full article can be found at:
'Prove you are not a robot': how the Captcha scam captures your computer | Money | The Guardian

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.

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