

From mountain to sea

Trading Standards Scams Bulletin No. 133

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

Nothing to report.

Protecting Our Community

Aberdeenshire Trading Standards have taken a number of concerning reports over the last two weeks from residents in the Kincardine area about a company called RD Road Resurfacing Ltd. This company is known to travel the length of Britain looking for work.

The reports centre on employees attending at rural homes over the last couple of weeks and offering to resurface private roads between those homes and public roads. On more than one occasion work has been done and residents have paid many thousands of pounds, only to find that the standard of work done is extremely poor, with little more than a very thin layer of surface dressing laid, dressing which is already breaking up and the original surface showing through.

Other areas of concern were the workmen starting work without permission and failing to provide customers with cancellation rights.

If these workmen attend your home, our advice is to remain polite but firm, state clearly "Thanks, but no thanks", don't be drawn into discussions about money or prices, simply withdraw from the conversation as quickly as possible, then close and lock your door.

From mountain to sea

Trading Standards also request that any contact with this company be reported to us via Consumer Advice Scotland on 0808 164 6000. Our enquiries are still ongoing and we are liaising with affected residents.

Scams etc.

Phone Scam

Aberdeenshire Trading Standards have been made aware that a small number of residents in the Turriff area have recently received phone calls from callers purporting to be working for a company called Uptel. The callers claim that they're calling about a switchover from the old copper wire system to the new digital network.

However, these callers have gone on to ask residents some very personal questions such as mobile phone numbers and e-mail addresses; questions which are completely inappropriate for genuine callers working for telephony companies. On one occasion, an elderly resident was asked by the caller to permit them remote access to her iPad in a call which lasted nearly an hour. Thankfully, a family member came home in the nick of time and stopped the process immediately.

Needless to say, these calls are a scam. It also appears that the callers are deliberately targetting elderly and/or vulnerable people, it would appear to obtain their personal details of financial data, to commit further crimes.

Some points to consider:

- The only telephony company with a name similar to Uptel was dissolved in October 2020,
- The digital switchover is being handled by large companies like BT, Virgin, Sky, O2 and Talk Talk, not by the smaller companies, even the genuine ones,
- Further information about the switch over can be found [here](#),
- Please, never divulge personal information or, more especially sensitive data like bank card or credit card information, to cold callers, no matter who they say they are. You only have their word that they are genuine. Make them work for it; let them tell you why they called and for them to provide you with the information these companies should already hold about you, which you can then confirm or refute. Don't make it easy for scammers to cheat you,
- Likewise, never divulge any log on information to any cold callers or allow them access to your digital devices as they may access areas they should not and steal sensitive information like bank account and credit card details which they may use to financial commit crimes, at your expense,



From mountain to sea

- Phone scams are so prevalent these days that it is wise to be very cautious with every call you receive until you can be sure that you know exactly who you're speaking to,
- If in any doubt, simply hang up without getting in to a conversation with the caller as they may use this as a way to try to break down your resistance or extract information from you. Remember it's "Thanks, but no thanks", then simply hang up,
- If you are persistently pestered by scam or spam calls, please consider a call blocking device if you're still on copper wires or contact your telephony provider about their call interception services if you're on the new digital network. They may be a small charge for the interception service,
- Please also remember to report these matters to your local Trading Standards office.

Misc.

I am obliged to my colleague Gordy Macdonald at Police Scotland's Cybercrime Unit for bringing the following e-mail scam to my attention:

Fake US Police department e-mail scam

It is reasonable that every person and organisation connected to the internet should, at some stage, expect to receive a scam email, text or message. This is a constant threat which universal connectivity brings and, due to the ease and minimal technical skill required, phishing attacks can be targeted at numerous online connected websites and accounts with ease.

This being the case it is essential we are prepared when we receive a phishing e-mail, in being able to detect, deter, respond to and recover from any consequences, but also to share awareness to support and protect others.

Recently, cybercriminals set up a fake US Police Department website calling itself the Utopia Police Department. The cybercriminals then sent out a series of scam e-mails from this site, initially targeting residents local to that area in Texas USA.

The scam e-mails, understood to have originated from a different country, were written with authority and urgency, in terms of an ongoing enquiry and reference to recipients of the e-mail obstructing the law if they did not provide their personal information including bank details and home addresses, placing them under duress and confusion.

From mountain to sea

Law Enforcement in the area have issued local awareness of this threat and for recipients not to respond. Such is the reach of online connectivity it is understood similarly titled scam e-mails have now been received by organisations in Scotland.

As a result, we can share wider awareness of this scam in order that you are informed and prepared in terms of your response should you receive a scam e-mail, text or message.

Responding to a scam or phishing e-mail is a process which, for some, may sound daunting as they can affect us and our response in different ways. To offer support, the guidance [here](#) from our trusted partners at the NCSC (National Cyber Security Centre) will help you with a structured approach to spotting and reporting scam e-mails, texts, websites and calls.

If you have received an e-mail which you're not quite sure about, you may also forward it to report@phishing.gov.uk even if you are not certain it is a scam. Please note that you are not formally reporting to Police via this option – you will have to do that separately.

It is important to note that Police Scotland will never send out e-mails asking for recipients to provide personal or banking information of any kind.

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101.

Comment:

In short, if you receive an e-mail from Utopia Police Department, it is a scam. Please forward it to report@phishing.gov.uk, then report the matter to Police Scotland on 101 or online by clicking [here](#).

Stop Press

I am obliged to a resident in the Kincardine area who drew my attention to the following news article (he knows who he is) about Booking.com. This is the same resident who reported the booking agency confirmation scam referred to in Bulletin 130. The first 'confirmation' scam was reported to Aberdeenshire Trading Standards back in early February by a resident in Turriff and featured in Bulletin 128. Booking.com was the booking agency referred to in both Bulletins.

The latest report refers to an article in The Guardian on Monday 13th April which advises that Booking.com has just alerted customers that its database has been

From mountain to sea

hacked and their personal data accessed by the hackers. Booking.com also states that “financial information was not accessed”.

Should any of our readers receive any e-mail or WhatsApp messages from Booking.com (especially if the message comes from a mobile number with the prefix +316) after making a booking through that company, where the message asks to confirm a booking and refers to additional payments, even temporary ones, and that you should act with urgency to secure the booking, please do not simply follow the instructions in the message as it may be from these hackers and please do not reply to it. Do not panic; take a moment to think about things.

Instead, contact your accommodation provider or venue directly to confirm the booking with them. If they confirm that the booking is safe and they do not require further confirmation, report the matter to Booking.com (using a phone number, e-mail address or webpage you have sourced yourself, not one from the suspicious message), if you are so minded to do so.

Please also remember to report the matter to your local Trading Standards office, so that we can alert others.

You can read the full article here:

[Booking.com warns customers of hack that exposed their data | Hacking | 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



From mountain to sea

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 tradingstandards@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](#).