Aberdeenshire COUNCIL

From mountain to sea

Doorstep Callers and Scams Bulletin No. 101

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.

Scams etc.

E-mail scam

One notable e-mail scam which landed in our Trading Standards Inbox and which we've seen in numerous other Inboxes and Spam folders recently is doing the rounds at the moment. It's a particularly disturbing e-mail which has as the command line 'You have been hacked' and it appears to have been sent from the recipient's own e-mail address. Clearly, it's intended to alarm.

The body of the e-mail then opens with the words 'Hello pervert' and goes on to advise that the sender of the e-mail has installed a spyware programme called Pegasus on all of the recipient's devices and that the sender has recorded the recipient watching pornography on the internet through the relevant device's camera. It is also clear that the e-mail is aimed at men.

The sender goes on to say that they have accessed all of the recipient's contact details and that unless the recipient deposits $1300's worth of Litecoin (a cryptocurrency) into the sender's Litecoin wallet within 48 hours, the sender will distribute video of the recipient watching pornography to all of their contacts. If the money is paid, the sender promises that the videos will be permanently deleted. The sender then advises how to buy Litecoin.

The final part of the e-mail is a list of 'do nots', such as do not reply to the e-mail, do not report the matter to the Police and do not re-set or destroy the 'affected' devices as the sender will know from monitoring the devices through Pegasus.

This is a particularly grubby type of scam which, along with others of its kind, is often referred to as sextortion. Reporting rates for any type of sextortion are particularly low due to the delicate nature of the allegations and the possible embarrassment a victim might feel in reporting the scam to enforcement agencies.

Some points to consider:

- The tone of the e-mail is very overbearing and threatening, designed to make the recipient feel that they are powerless, trapped and have no other option but to comply with the instructions sent. This is deliberate manipulation by the sender,
- There is a genuine piece of spyware called Pegasus but its creators say is only sold to governmental security and law enforcement agencies for specific purposes which do not include extortion,
- The use of the word 'program' in the message, as opposed to the UK variant of 'programme' and the reference to payment of $1300 (with no qualifier such as AUD (Australian dollars), NZD (New Zealand dollars), CAD (Canadian dollars) etc. suggests that this scam originates in the US,
- These types of e-mails are sent out to huge numbers of people all at once, with the aim of snaring a small per centage of recipients into making payment and netting the sender large sums of money. They are effectively a 'shot in the dark' and are playing a numbers game,
- The truth of the matter is that there will be no spyware on recipients' devices so scanning these devices with anti-viruses and other security programmes will result in them not finding anything,
- For obvious reasons, some people will be panicked into making payment. Given the above points, they should NOT do so,
- Instead, recipients should report the matter to the National Cyber Security Centre by forwarding the e-mail to the e-mail address report@phishing.gov.uk for the NCSC to collate and act against,
- Then place the e-mail into the Spam/Junk folder on your device and, if you can, block the sender,
- Further advice about dealing with sextortion can be found on the Victim Support website by clicking here,
- The only valid point this e-mail makes is "don't be so careless about your online security". Whatever security programmes or suites you have on your devices (anti-viruses, firewalls, pop-up blocker etc.) please make sure you know how to use them and that you keep them up to date. This

can usually be done with least effort by setting them to install updates automatically.

As always, please contact your local Trading Standards office if you need any advice about scams like this one.

Misc.

BT Enhanced Call Protect

In a recent bulletin we mentioned the use of AI by companies seeking to make contact with consumers. This generated some feedback from people concerned about the use of AI. However, there is another side to AI usage as the following article illustrates.

In May 2024, BT introduced a new service called Enhanced Call Protection for customers on their Digital Voice service. Since that time until the beginning of October 2024, Enhanced Call Protection has intercepted almost 2.5 million scam calls and identified a further 17 million+ spam calls to their customers. In one day, it blocked more than 46,000 scam calls – all done by an AI powered system provided by a partner company called Hiya.

The system works by flagging up a call on the phone's display panel with the words "Nuisance?" and the resident can then decide to accept or reject the call. If they accept, the resident then speaks to the caller but if they reject, the call is diverted to the resident's spam voicemail inbox.

The service is completely free to all BT customers who move over to the Digital Voice service and it is only to be hoped that something similar will be introduced by other telephony providers in the near future.

Further information about Enhanced Call Protection can be found on the BT website by clicking here.

Aberdeenshire COUNCIL

From mountain to sea

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 the Consumer Advice Scotland website or call them 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.

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.