Aberdeenshire COUNCIL

From mountain to sea

Doorstep Callers and Scams Bulletin No. 74

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 to Trading Standards Scotland, please click on the Trading Standards Scotland Bulletin page.

Doorstep Callers

Nothing to report.

Scams etc.

E-mail scam #1

One resident of south Aberdeenshire recently reported to Trading Standards about a scam e-mail he had received. The e-mail purported to come from HMRC advising that the resident was eligible to receive a tax rebate of £550. All that was required was that he should click on a hyperlink in the e-mail to start the process of claiming.

Although at first glance the e-mail is quite convincing, compared to the normal HMRC e-mails there were some discrepancies:

- In a genuine e-mail the first line consists of a white crown on a black background and the words 'GOV.UK' in white capital letters. In the scam e-mail the first line had no crown and the lettering was light gray,
- On the second line the genuine e-mail has a black crown on a white background and the words 'HM Revenue and Customs', the scam e-mail has '@HMRC Payment conformation',
- In the third line of a genuine e-mail the recipient is named, on the scam e-mail it reads the impersonal 'Dear Customer',
- In a genuine e-mail, the tone of the text is quite direct 'your latest tax calculation' (calling a spade a spade), in the scam e-mail the flowery euphemism 'your last annual fiscal activity' is used (a popular trend in north America),

- In the genuine e-mail, HMRC advises 'For security reasons we have not included a link with this e-mail'; in the scam e-mail a link is included,
- Hovering a computer's cursor over this hyperlink shows a web address for a site called 'burdwancardbank.org' rather than a web address for the usual 'gov.uk' website,
- Although the e-mail appeared to come via the Government Gateway, a closer look revealed that the e-mail had actually come from an '@optonline.net' e-mail service (a 'popular' e-mail service provider) rather than a 'gov.uk' e-mail address.

Taken together, the observant recipient would realise quite soon that although it is better than the usual attempt, with the above details and other more minor discrepancies, this is a phishing e-mail designed to catch out the unwary; the £550 refund does not exist (it is simply bait) and the hyperlink would lead to someone being asked to input personal details which would then lead to a financial loss for the recipient or their personal data being stolen and misused by other scammers.

E-mail scam #2

Around the same time, a resident of north Formartine reported that she'd received an e-mail advising her that her automatic TV Licence renewal had hit a snag. The e-mail went on to say that the snag may have been due to a change in banking arrangements and it provided a hyperlink in the text for the resident to click on, to set things right and set up a new Direct Debit.

However, as the resident is a reader of these bulletins she was already wary and noted:

- The sender's e-mail address was one which bore the suffix '@skynet.be' (another 'popular' e-mail service provider) rather than the official e-mail suffix of '@tvlicensing.co.uk',
- The e-mail was addressed in the first line of text to the recipient's e-mail address rather to her as a named person,
- The general layout of the e-mail was poor, the graphics were very plain and there were a couple of obvious spelling mistakes in the text of the message,
- By hovering the computer cursor over the hyperlink, a new web address became visible. This one had the suffix '.com/ar', which suggests a business based in Argentina rather than TV Licensing in the UK.

Needless to say, the resident did not click on the link and provided no details for a Direct Debit.

Some points to remember when dealing with suspect e-mails:

- Hovering your computer's cursor over the sender's e-mail address can often disclose another e-mail address. If this happens, it's likely that the e-mail address you first saw is not the sender's but has probably been spoofed,
- Likewise hovering the cursor over any hyperlink in the text of an e-mail can show the web address of the hyperlink, usually down in the bottom left corner of your computer screen,
- NEVER click on a hyperlink in a suspect e-mail, it will undoubtedly lead to a scammer trying to steal your money or your personal data,
- If you can, send the suspect mail on to the National Cyber Security Centre via their spam e-mail address of report@phishing.gov.uk so that the NCSC can investigate it,
- Then, send the e-mail to your e-mail provider's Spam or Junk folder.

If you think that you have been the victim of a scam e-mail, particularly of you've lost money or believe your personal details have been misused and you live in Scotland, please report the matter timeously to Police Scotland. Many sources of advice about scams tell people to report these e-mails to Action Fraud, but this is only for people who live in England, Wales and Northern Ireland. Action Fraud does not cover Scotland.

Misc.

In Bulletin no. 73 we reported an incident involving a resident apparently having unsafe overhead power lines and how these can be dealt with. This generated a reader to ask if the same service is still offered by BT Openreach. Having spoken to a BT Openreach Engineer, we can confirm that if anyone is concerned about potentially unsafe overhead telephone lines or other infrastructure, they can still report the matter to BT Openreach who will be happy to take the necessary action. This can be done by phoning the BT Operator on the phone number 150.

We should also point out that, as advised in Bulletin 73, as well as obtaining the phone number for your electricity supplier from your bill, you can also call the 105 phone number to report dangerous power lines.

Also from Bulletin 73, we received a question about the trueCall Call Blockers which were being provided free of charge by Friends Against Scams and their compatibility with the new digital/internet phone lines. We have raised the matter with trueCall and been advised that (in simple terms) that their Call Blockers are compatible with these new phone lines. All that is required is that the Call Blocker is plugged into one of the router/modem's phone sockets and a traditional phone (pre-digital) is plugged into the Call Blocker. When a known

phone number calls, that call is put straight through to the resident as the phone number is on the Call Blocker's safe list. When an unknown phone number calls and asks to speak to the resident, only the traditional phone will ring, alerting the resident that it is an unknown number. The resident can then choose to answer or not and then choose to put the number calling on a safe or blocked list by the press of a single button on the phone. In either scenario, with this set-up, all safe calls can be answered on any phones in the house. Only unknown calls should be answered on the pre-digital phone, to allow the resident to classify the number calling, for future reference.

It should also be remembered that the effectiveness of these devices comes from them intercepting unknown callers with a pre-recorded message telling the caller that high-pressure sales calls are not welcome and that calls from these numbers can be blocked from then onwards by simply pressing the 'hash' key on the device. Silent calls and pre-recorded message cannot get through as the caller has to verbally identify themselves before they are permitted to speak to a resident.

Little Book of Phone Scams
Police Scotland have recently made available a short booklet about phone scams, called the Little Book of Phone Scams, which can be viewed or downloaded from the Police Scotland website here.

This booklet illustrates some tactics used by scammers and offers some very useful ways to spot these scams and how to avoid falling victim to them. Please share it freely.

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.

Aberdeenshire COUNCIL

From mountain to sea

Contact Info

For non-urgent Trading Standards enquiries in Aberdeenshire, please contact Consumer Advice Scotland at https://www.consumeradvice.scot/ or 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 Friends Against Scams at https://www.friendsagainstscams.org.uk/ or Take Five at https://takefive-stopfraud.org.uk/

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

All previous Trading Standards bulletins can be found at: http://publications.aberdeenshire.gov.uk/dataset/trading-standards-crime-and-scams-bulletin