Cold Calling Alert – Doorstep cold callers offering driveway work

We are warning residents to be on their guard after receiving reports of doorstep cold callers approaching residents in the Aylsham area offering to undertake repair work or to lay new driveways.

Trading Standards advises when looking to have work done on or around your property only deal with reputable companies you have researched and chosen yourself and have obtained a written quotation from.

Anyone concerned about doorstep cold callers in Norfolk can contact us through our partners the Citizens Advice consumer helpline via their online reporting form or by telephone on 03454 04 05 06.

Looking for a Trader you can Trust? Try a Norfolk Trusted Trader. To search our directory and read feedback from their customers visit www.norfolk.gov.uk/trustedtrader

Scam Alert – Emails attempting to 'blackmail' the recipient

Norfolk residents have told us about emails which attempt to blackmail the recipient.

The emails often state they have 'hacked this mailbox' or have been 'observing you online' and sometimes include a password that will be known to the recipient.

The emails will often make claims to have 'access to all your accounts, social networks, email, browsing history' and 'all your contacts, files from your computer, photos and videos' and often make accusations about websites you have visited. It then threatens to share this with your contacts unless an amount is paid in Bitcoin.

Action Fraud offer the following advice regarding this type of email and how to protect yourself:

- Don't reply to the email or be pressured into paying: it only highlights that you're vulnerable and you could be targeted again. The police advise that you do not pay criminals. Try flagging the email as spam/junk if you receive it multiple times.
- Perform password resets as soon as possible on any accounts where you've used the password mentioned in the email. Always use a strong, separate password for important accounts, such as your email. Where available, enable Two-Factor Authentication (2FA).
- Always install the latest software and app updates. Install, or enable, anti-virus software on your laptops and computers, and keep it updated.
- If you have received one of these emails and paid the fine, report it to your local police

force. If you have not paid, report the email as a phishing attempt to Action Fraud using their online form or by telephone on 0300 123 2040

Scam Alert – Further reports of emails claiming to be from 'TV Licensing'

We have received more reports from Norfolk residents about email claiming to be from TV Licensing.

These emails generally claim that TV Licensing have been unable to take a payment, that there are issues with Direct Debits or that you are due a refund on your TV Licence.

The email then offers a link to enable you to make a payment or claim the refund. This link then goes to a 'genuine looking' version of the TV Licensing website which attempts to gather personal and financial information.

In some cases when people have submitted information to the fake website they are then targeted by telephone cold calls claiming to be from the 'Fraud Department' at their bank stating there has been 'fraudulent activity' on their account and they need to transfer funds to a new 'safe account' that has been set up for them.

Action Fraud report that since April 2018 victims of this scam have lost over £830,000.

We always advise to be very wary of approaches made in unsolicited emails and by telephone cold calls and remember:

- Never answer unsolicited emails, click on links or open attachments
- Don't assume a phone call or email is authentic even if they know basic details about you
- Always question unsolicited requests for your personal or financial information

TV Licensing have issued the following advice:

TV Licensing will always:

- Use donotreply@tvlicensing.co.uk (or donotreply@spp.tvlicensing.co.uk) to email you
- Include your name in our emails (unless you told us you don't need a licence and didn't provide a name)

TV Licensing will never unprompted:

- Email you to ask for bank or personal details
- Email you to tell you that you're entitled to a refund
- Offer you a discounted TV Licence

TV Licensing will never ask on their website for:

- Your card details to take a missed payment before we've first asked you to sign in to identify yourself using your licence number, surname and post code
- Your mother's maiden name
- Your date of birth (unless you're 74 or over and applying for a free TV Licence)
- You can read further information about spotting scam TV Licensing email on the TV Licensing website

You can report scam emails to us via our partners the Citizens Advice consumer helpline on 03454 040506.

If you have responded to one of these emails and have submitted bank details or card numbers on a linked website, contact you bank immediately on the number printed on your card.

Scam Alert – 'International Postcode Online Lottery' letters

We have received reports about letters claiming to be from the 'International Postcode Online Lottery' being received by Norfolk residents. The letter states the resident has been awarded a prize of £900,000 in a recent draw made in 'Melbourne, Australia'.

These letters are a scam and no prize is available.

If you receive this type of letter dispose of it correctly without responding in any way.

Here are some simple steps you can take to avoid lottery scams:

- If you haven't entered a lottery then you can't have won it. Never respond to unexpected communications
- Official lotteries in other countries operate in much the same way as the UK's National Lotto. No official lotteries that we know of contact people to tell them of their win.
- We don't know of any official lottery operators who ask for fees to collect winnings. Any request for a fee payment is a good indication that someone is trying to scam you.
- Never disclose your bank details or pay fees in advance to claim a lottery win
- If they've provided an email address to respond to, be very suspicious of addresses such as @hotmail.com or @yahoo.com or numbers beginning with 07 because these are free to get hold of
- Genuine lotteries thrive on publicity. If they ask you to keep your win a secret it's likely to be a scam.
- Many examples of lottery scam letters have bad spelling and grammar – see this as a warning that fraudsters are at work