



JULY/AUGUST NEWSLETTER 2018

A message from Trading Standards



Suffolk residents are being urged to remain vigilant in regards to doorstep traders offering green energy solutions

Often they may see your solar panels and approach you, claiming to be the company who installed your panels. They may then advise that you need to purchase additional products, or offer a free 'health check'

They will then use the allure of a free health check to sell you a new system, and have been known to tell consumers that the emergency services will not visit your property unless you purchase additional items. This is a lie

If you have concerns about someone visiting at your door, call us via 03454 04 05 06 or Suffolk Police on 101.



Minutes from the 2018 Annual General Meeting are available from our website.

Thank you to those of you that came along to the 2018 AGM at Woolpit.

Please take time to read the minutes, as it gives a comprehensive account of the past year, and highlights the requirements for the year ahead.

The key message still remains that your help is needed - the Executive Committee is looking for more volunteers to get on board. So if you have around 4 or 5 hours a week, typically in your own home environment and are interested, please get in touch.

Roles and descriptions can be viewed on our website [here](#).



Never pass on your bank details

A co-ordinator from the Lowestoft area had a recent phone call, from two young men with English accents, (possibly Home Counties), purporting to be from BT.

They sounded very plausible, offering a good discount to reduce line rental, broadband etc. and as a direct debit customer, in order to “complete the paperwork”, they needed bank account number, email address and a mobile number in case the telephone system “collapsed”.

No personal details were given out, but because the caller had been convincing, the co-ordinator rang BT to check on the validity of the offer. BT confirmed that no such offer existed and they had not contacted the co-ordinator at all.

Action Fraud

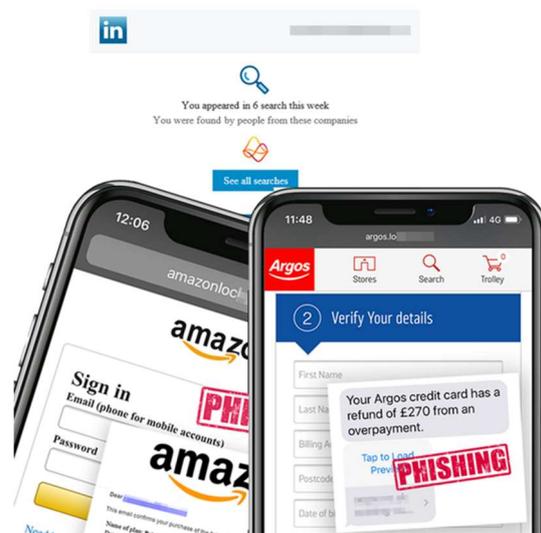
Report Fraud & Internet Crime

0300 123 2040

LATEST PHISHING ALERTS

Watch out for these fake emails and text messages

Action Fraud have received multiple reports about fake emails and texts from the likes of LinkedIn, Amazon, and Argos.



The LinkedIn message claims that your profile has appeared in multiple searches and provide links you can click on to get more details. These links lead to malicious websites designed to steal your personal and financial details.

With the Amazon messages, the subject line and content of the emails vary, but they all contain links leading to phishing websites designed to steal your Amazon login details.

Fake text messages purporting to be from Argos claim that you're owed a refund. The link in the messages lead to phishing websites designed to steal your personal information, as well as payment details.

Always question unsolicited requests for your personal or financial information in case it's a scam. Never automatically click on a link in an unexpected email or text.