

## Consumer Alerts – February 2022

### **Beware traders offering to power wash roofs.**

A householder in Thornton Cleveleys was left with a patchy roof, loose ridge tile cement, blocked drainpipes and sludge over her driveway, after agreeing to pay £500, which then became £850 within a day, to have her bungalow power-washed. Lancashire residents are warned to take heed of this case, and to be careful of taking on cold calling roof cleaning companies.

If you have a problem with moss on your roof, seek the advice of a roofer to find out the best solution. Use local known reputable traders, ask for recommendations from family or friends and get more than one quote.

Always check that you have a full address for any trader you deal with, and that all the work to be done and price to be paid are obtained in writing before the work starts. If a contract is agreed at your home, you should usually receive 14 day cancellation rights in writing.

**Trading Standards advice is to always say no to cold callers. The Safetrader scheme can help you find a trader in your area, contact 0303 333 1111 or go to [www.safetrader.org.uk](http://www.safetrader.org.uk)**

### **Scam 'winter payment' email**

Reports have been received of a scam email doing the rounds alleging to be from E.ON headed 'winter payment confirmation'. The email states 'Our system indicates that an error in our billing procedures has led to an overcharge on your latest payment to us'.

In one instance the recipient was advised they were eligible for a refund of £85 and invited to click a link to 'view here'. The link takes you to a website in India not associated to E.ON.

This is a phishing email, E.ON will never ask you for personal information such as passwords, payment details or your address. Phishing emails can be forwarded to the National Cyber Security Centre at [report@phishing.gov.uk](mailto:report@phishing.gov.uk)

### **Scam email requesting a survey be completed**

Beware receiving an email claiming to offer a £90 'promo reward' from the retailer Currys in return for completing a survey. An unsolicited email is received branded as if it is from Currys asking people to click through to a 'marketing survey' in return for the 'reward'. Clicking on the link can provide an opportunity for scammers to steal your personal information.

### **WhatsApp 'Hello Mum' scam**

Please be extra vigilant and cautious if you use WhatsApp. A current scam contacts you from WhatsApp using an unknown number beginning with 'Hello Mum' or similar, pretending to be your daughter or a family member and explains they have recently lost their mobile phone, hence the unknown number, and are struggling to use online banking and have an urgent bill that needs paying. The scammer, whilst stating they are ashamed to ask, proceeds to ask for the owed money to be transferred to an account, the scammers account.

### WhatsApp pass code scam

In another WhatsApp scam, beware of receiving a text containing a 6 digit WhatsApp code that you were not expecting and have not initiated. You would usually need this code if setting up a new WhatsApp account or logging in to your existing account on a new device.

If you have not initiated this request it could be a scammer trying to get access to your WhatsApp account. The next step in the scam is for the scammer to message you in WhatsApp, the message would look as if it has come from one of your known legitimate contacts, asking for this 6 digit code.

Be very suspicious if you receive such a request via WhatsApp from a friend or family member, it is likely a scammer has hijacked your account. Never pass any 6 digit security code you are sent to anyone including close friends and family members.

### WhatsApp phishing scam

In yet another WhatsApp scam a Lancashire resident received a message from a friend who had passed away a few years ago. The message was a link to click on. This is a phishing scam, and may well have been sent without the scammer knowing the sender had passed away, the link if clicked on would no doubt take you to a site asking for personal details.

Be very cautious about clicking on a link that seems suspicious or unusual. In this case the receiver found the scam very upsetting but luckily did not click on the link.

**Contact the Trading Standards Service via the Citizens Advice Consumer Helpline on 0808 223 1133**

**Further information about current scams can be found on our Facebook page, [www.facebook.com/StanleyDards/](https://www.facebook.com/StanleyDards/)**