

MONTHLY FRAUD UPDATE – November 2021

For the information of all Southend Borough Council staff and the public to enable them to protect themselves, their families and the Council against the most current threats from fraud and cybercrime. Please feel free to distribute these messages to anyone you feel may benefit from them.

Hi All

I realise this is a bit late and I can only blame my workload. Please note that due to my annual leave there will be no fraud update in December and my next issue will be at the end of January 2022.

Online shopping

I know that Black Friday has come and gone but we are now deep into the annual Christmas online shopping frenzy. This is a lucrative time of year for scammers search for hard-to-find items or the best deals.

Social media platforms, online market places and auction websites are increasingly used by criminals to scam shoppers, by getting them to pay in advance and then not delivering the goods or services.

It has been reported that there has been a rise in these scams with criminals exploiting those looking for common online gifts such as games consoles, bicycles and clothing. Other scams involve home improvement and DIY purchases such as patio heaters and sheds as criminals adapt to more people staying at home and choosing to invest in their home environment.

When considering buying from a website, particularly one that you don't know, take a minute to think about it, do some research: has anyone reviewed the website or online shop? A couple of quick checks could save your money. On auction websites, check that they are legitimate and then check the product reviews (I always go straight to the one-star reviews, it can be sobering).

Scam websites often focus on the most popular, expensive or hard to find items of the season. If everywhere else is sold out or if it is way cheaper than anywhere else, take a minute to think and be very suspicious.

REMEMBER: If it's too good to be true then it probably is.

A guide to safe online shopping can be found [here](#).

DVLA scams

The DVLA have warned of a raft of new scams via text and email messages claiming to be from them. The DVLA will never ask you to reply, give personal or bank details or ask you to log into an account.

The new scams include:

- A final request for you to contact them by clicking on a link.
- An offer to claim a refund for overpaid vehicle tax by clicking on a link.
- A notice of unpaid vehicle tax with a link to sort it out.
- A notice that your not up-to-date with your vehicle tax again with a link.

OFFICIAL



Needless to say, DO NOT CLICK ON LINKS in texts and emails. If you are concerned contact the DVLA using the numbers on their [website](#).

Lottery fraud

Lottery fraud happens when criminals use fake messages and calls to convince you that you have won a lottery or prize draw. They then ask you to pay and advance 'fee' so that you can receive the winnings. Often they ask payment in the form of gift cards and which you are then asked to provide the codes to the fraudster. Sometimes they ask for your personal or bank details in order to give you your winnings.

What they really want to do is steal your money.

Personally, I hang up on an unsolicited call about the time they have finished their first sentence. I do not feel that I have lost out on anything as a result.

Now the evenings are drawing in

It gets dark very early this time of year and, although I know this is not fraud I will say it anyway, this is a great time for burglars, particularly with the prospect of gifts in the house.

Make sure you lock up at night, use light timers or leave a radio on in the rooms you use the most. Burglary is generally an opportunist crime and they are looking for unsecure or empty properties to attack.

You can find out more about protecting your home [here](#).

WhatsApp scam

These are on the increase as fraudsters continue to innovate sophisticated ways to deprive you of money. A popular scam is to compromise or hack someone's WhatsApp account and then message friends or relatives for money. Sometimes they will use an unknown phone number and claim to have lost their phone.

If you receive such a message from a friend or relative, if they are in need, it is worth a phone call. If a contact asks you for personal information, money or a six-digit code (this could be used to hijack your account) verify it independently; talk to the sender.

Stay safe and have a wonderful festive break and I hope that the New Year brings you all success and happiness.

Kind regards

Shaun

OFFICIAL

REMEMBER, IF IT'S TOO GOOD TO BE TRUE, THEN IT IS.



'Tell2 over a brew' is a communication initiative that empowers you to discuss crime prevention messages with others in your life, who otherwise may never know. Start with 'tell2' and ask them to do the same. An unbroken chain of 26 tell2'ers would reach 67 million people. It starts with YOU!



'Take Five' is a national campaign to offer straight-forward, impartial advice that helps prevent email, phone-based and online fraud – particularly where criminals impersonate trusted organisations. Find out more at www.takefive-stopfraud.org.uk.

If you suspect someone is trying to defraud the Council call the Counter Fraud & Investigation Team on 01702 215254 or email us at counterfraud@southend.gov.uk.

If you or someone you know is vulnerable and has been a victim of fraud, please call Essex Police on 101.

Report fraud or attempted fraud by contacting Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.