

MONTHLY FRAUD UPDATE – March 2022

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.

Holiday frauds

Now that the restrictions are easing and the Summer seems at last on its way, many of us are starting to think about holidays and short breaks.

Please do thorough research into flights, package holidays and accommodation to make sure they're legitimate. Criminals look to take advantage of you by advertising 'too good to be true' offers or prices.

Look for reviews from reputable sources before making any bookings or payments. You might also confirm if an accommodation really exists by verifying the address through web searches and online maps. This might seem like a lot of extra effort, but can you afford to lose your money?

Where possible, use a credit card when booking as these carry a lot more protection for you.

Remember: If it's too good to be true, then it is.

HMRC scams

Impersonating HMRC continues to be popular with scammers and, now that the end of the tax year is approaching, this is expected to increase. This often takes the form of fake emails or text messages appearing to be from HMRC claiming you are due a tax refund or urging you to provide personal and financial details. If in doubt, confirm directly with HMRC.

Criminals may also offer their services to assist you with a refund application or self-assessment while charging a fee to complete the process (while stealing your details).

It is OK to say no to unsolicited offers of help or requests for your information. I refuse all such approaches and have not missed out.

NHS scams

Scam warning

- Be aware of personal information in messages claiming to be from the NHS.
- Be alert to links or attachment in unexpected messages claiming to be from the NHS.
- Do not respond to requests for money, bank details or passwords.

Remember

- The NHS will NEVER ask for payment or any financial details.
- If you are suspicious about an email forward it to report@phishing.gov.uk
- If you are suspicious about a text message, forward it to 7726 (it's free of charge).

For information on NHS coronavirus testing, visit www.nhs.uk



Ukraine frauds

There have been reports in the press of fake emails pretending to raise money for the victims of the war in Ukraine. The advice is:

- DO NOT click on links or attachments in suspicious emails or respond to unsolicited messages asking for personal or financial details, even if they are in the name of a charity.
- To donate online, go directly to the charity's website rather than clicking on a link.
- Be cautious about donating to an online fundraising page: fake ones are often badly written or contain spelling mistakes.
- Be wary of emotional online posts from fraudsters pretending to be victims of the war and asking for money.

There have also been variations of a common scam where an individual claims to be a Ukrainian businessman trying to move money out of the country, and who needs to use a bank account outside the country. If you provide account details, they will then drain it.

Read more from BBC News [here](#) and [here](#).

Secure, protect, prevent

Not fraud, I know, but sound advice from Essex Police.



OFFICIAL

If you can reach over and unlick your gate, so can they. Putting locks on all gates which access your garden will help make your property more secure. Make sure the locks cannot be reached from the outside.

I would add that the security of your sheds and outbuildings is also important, not only to keep your stuff safe but often there are tools inside that could be used to break into your house.



Burglars have been known to use rubbish bins and other items lent against fences to gain access to houses. If you can, store your bins in a secure location, away from fences and any garden access gates.

Essex Police provide advice and information about fraud can be found [here](#).

Kind regards

Shaun

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.

OFFICIAL

OFFICIAL

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.