

MONTHLY FRAUD UPDATE – January 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.

I hope the holidays treated you well and everyone was healthy and safe. There's quite a lot to get through from this month so I will try to be brief but informative.

Burglary

Essex Police are reminding residents that with darker nights still with us and many returning to work now, our homes are targets for opportunist burglars. Giving the 'illusion of occupancy' i.e., with lights that come on with a timer, is a proven deterrent.

Cloned Company scams

This is a form of investment fraud where fraudsters replicate real company websites using genuine details and advertised on search engines and social media. They promise an attractive return on investment but not so much that it is unbelievable. One such scam, cloning a popular comparison website, managed to defraud people of £750,000. The National Economic Crime Centre gives this advice:

- Reject unsolicited investment offers however they are made (online, social media, or on the phone). Be cautious when dealing with large sums of money even if you made first contact.
- Always check the Financial Conduct Authority's (FCA) register and warning list of firms to avoid.
- Only use the contact details on the FCA's register, not the one the firm gives you.
- Consider seeking impartial advice before investing.
- If you think you've fallen victim to investment fraud, report it to Action Fraud as soon as possible (details below)

Covid-19 scams

There remains a lot of text message scams telling you that you have been in contact with someone who has tested positive for the Omicron variant and telling you to pay for a PCR test.

PCR tests are free.

- Be wary of links and attachments in unexpected text or email messages.
- Do not respond to requests for money, passwords, or financial details.
- If you need a PCR test, book it through the NHS website.
- If you receive a call and suspect it might be fraud, hang up.

You can report a suspicious text message by forwarding it to **7726**, free of charge, and you can report suspicious emails by forwarding them to **report@phishing.gov.uk**.

Instagram fraud

There have been worrying reports in the press concerning the hijacking of Instagram accounts. Scammers have been able to impersonate one of the victim's friends telling them how they invested £500 and got £5,000 back. If they are interested, they are told to contact another person on Instagram where they are instructed to transfer the money. They are then told that if they provide more money, they would get a special £20,000 bonus. Before they get the money, they are asked to record a short video about how great the investment was. Lastly, they are persuaded to hand over their account ID and password. The fraudsters then hijack the account to spread the video and start all over again.

Of course, no money is paid, only lost. The trust is built at an early stage with the video and if the potential victim messages the friend to see if it's real, they get confirmation as the fraudsters now control the account.

If you have young adults who might be drawn in by such an offer, please educate them.

WhatsApp scam

This scam is more aimed at older users and involves a WhatsApp message, or sometimes a call or text, from someone claiming to be a family member asking for money. This 'family member', often a daughter or son, claims to be short of money or late paying bills and asks for money to be transferred into an account. They will claim that they have changed their phone or number.

If you receive messages like this, be sure to check with the relative who is asking for money by other means. The first thing would be to contact them on the number you already have for them or via email.

Do you sell items online?

Apparently, there is an app available that makes it look like a transfer has taken place when it hasn't. The app creates a picture showing confirmation of payment when no money has been sent. Make sure you receive the payment on your online banking account before sending items. It is also good advice to take photos of the items before you send them so you have proof of condition in case of a fraudulent claim.

Romance fraud

This continues to be prolific and profitable for fraudsters. Criminals will use fake profiles to build an online relationship with their victims using social media, dating apps and gaming sites. They use social media to target specific groups, particularly widows and divorcees. They will go to great lengths to gain trust and convince victims that the relationship is genuine before asking for money. These people are highly manipulative and persuasive so that requests for money do not raise alarm bells. But they should. Make it a rule that you do not give money to people you meet online.

Fraud advice and tips

Essex Police provide advice and information on all the above and more [here](#).

Kind regards and stay safe

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.

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.