Trading Standards Scams News

A round-up of the latest scams alerts

Leicestershire County Council

February 2022

Welcome….

to the latest edition of the Leicestershire Trading Standards Service scams newsletter. Here you will find details of the latest scams and information about how to protect yourself and report a scam.

Romance Scams

As more people will be looking for friendship and even romance at this time of year, fraudsters will be spending weeks researching and looking for targets before taking the time to gain their victim's trust, to eventually ask for money.

It is important that no matter how long you've been speaking to someone online and how much you think you trust them, if you have not met them in person, it's important that you **do not**:

- ⚠ Send them any money
- ⚠ Allow them access to your bank account
- ⚠ Transfer money on their behalf
- ⚠ Take a loan out for them
- ⚠ Provide copies of your personal documents such as passports or driving licenses
- ⚠ Invest your own money on their behalf or on their advice
- ⚠ Purchase and send the codes on gift cards from Amazon, iTunes or Google Play
- ⚠ Agree to receive or send parcels on their behalf (laptops, mobile phones etc.)

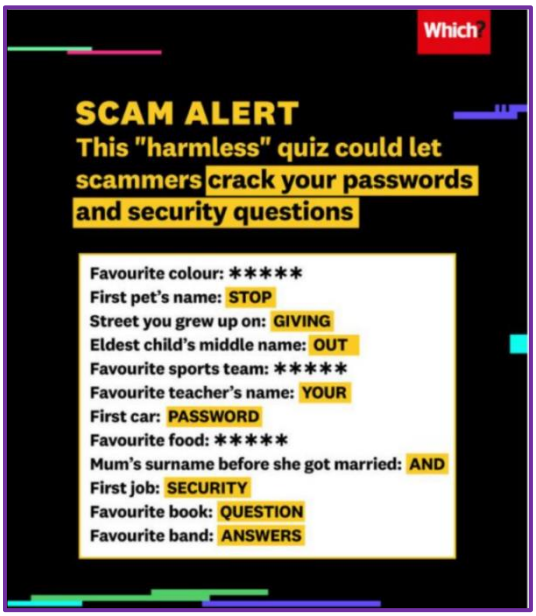
You can report suspicious dating or social media profiles, as the criminals behind them might not just be conning one person. Your report could help protect others.

If you think you have been a victim of a romance scam, do not feel ashamed or embarrassed - you are not alone. Contact your bank immediately and report it to Action Fraud on 0300 123 2040

For further information you can go to: https://www.actionfraud.police.uk/a-z-of-fraud/dating-fraud

---

Social Media Quizzes



A fun quiz pops up on your Facebook feed or another social media platform. A few questions are answered to prove how well you know a friend. Or a short personality test is offered to match with a character from a favourite TV show.

These quizzes appear to be meaningless, but the intent behind them is to collect information. Beware of questions like: "What was the first car you owned?" “What is your mother's maiden name?”. These are common security questions for insurance, banking, and credit card accounts. Sharing this information can lead to accounts being hacked, and personal and financial information being stolen.

This harmless quiz could let scammers crack your password and security questions and put you at risk of identity theft.

To find out how to further protect yourself go to: https://www.actionfraud.police.uk/a-z-of-fraud/identity-fraud-and-identity-theft

---

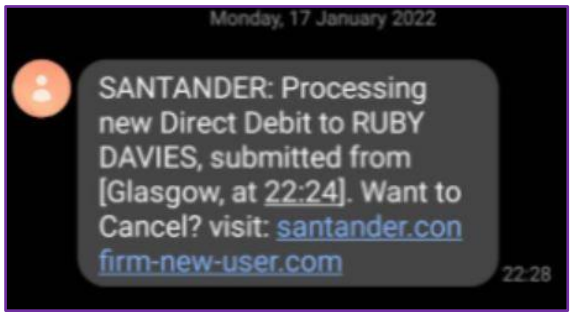
Suspicious Calls

Received a suspected spam text or call? All mobile customers using UK networks can report unwanted SMS messages or mobile phone calls to “7726”. The number is easy to remember as it spells “SPAM” on an alphanumeric phone keypad. This will allow your mobile provider to investigate the number and potentially block it, if it’s found to be fraudulent. These scams are usually aimed at encouraging you to hand over money, or your personal or financial information.

It can be hard to tell if a spam text or call is from a legitimate company or a scammer. Scammers could pretend to be from your bank or building society, or they might claim to be from your phone or broadband company.

Other examples include criminals claiming to represent HMRC, the NHS and delivery companies.

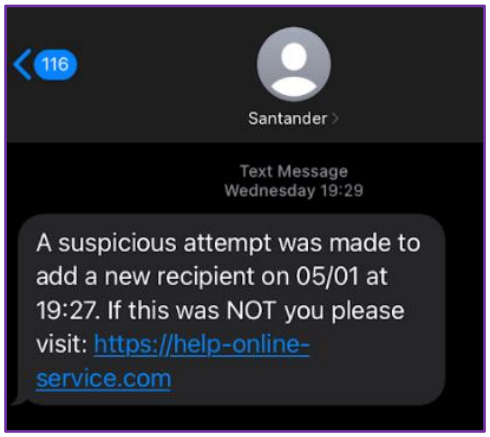
! Scam Alert: fake Santander 'new payee' texts !



Fake texts claiming to be from Santander are circulating, suggesting that suspicious 'new payees' have been set up on your account.

The first message tells the recipient that a 'new direct debit' has been established to a 'Ruby Davies' based in Glasgow. This name has presumably been made up entirely – the recipient had never heard of them, and the link is nothing to do with Santander.

The second message tells you that there has been suspicious attempt to add a new recipient on your account. Once again, the links take you to a site that's nothing to do with Santander.



Always remember:

⚠ Scammers can make a text message appear in a thread of genuine messages from Santander, such as previously sent One Time Passcode (OTP) numbers. This is easily faked and isn't proof that it's from Santander

⚠ Do not click on any links included in text messages or emails – instead contact your bank directly using the number on the back of your bank card, or through the 159 Stop Scams number.

⚠ If you do click on a link do not provide bank or security details and never download software on to your device.

⚠ You can report any suspicious text messages to your mobile network provider by forwarding the text message to 7726.

If you think you may have fallen victim to a fake text message, let your bank know via its genuine channels as soon as possible. Text messages and the formats used by banks are notoriously easy to clone, so these messages could be purporting to be from any bank.

Out & About…

Our Scams Liaison Officer has been out in the community to deliver scams awareness sessions to local groups. It's great to be able to go out and about again to meet the public in a Covid secure way. Scams talks mean we can offer face to face support again and to provide no cold calling door stickers and scams advice cards as well as giving residents the opportunity to pick up vital information about how to keep safe from scams.

If you would like to request a scams awareness talk for your local community group, you can get in touch via email at tradingstandards@leics.gov.uk

Finally,

If you would like to report a scam, you can get in touch with the following organisations:

Action Fraud – https://www.actionfraud.police.uk/

Citizens Advice Consumer Helpline - 0808 223 1133

To keep up to date with the latest scams information and advice, you can follow the Leicestershire Trading Standards Service Facebook page on: www.facebook.com/leicstradingstandards

Leicestershire Trading Standards Service
Tel: 0116 305 8000
Email: tradingstandards@leics.gov.uk
/LeicsTradingStandards