Trading Standards Scams News

A round-up of the latest scams alerts

Leicestershire County Council

August 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.

Cost of Living Crisis Scams…

New research by the Citizen's Advice has found over 40 million people have been targeted by scammers as the cost-of-living crisis takes hold. The most common types of scams reported included:

- Deliveries, postal or courier services (55%)
- Someone pretending to be from the government or HMRC (41%)
- Someone offering a fake investment or financial 'get rich quick' schemes (29%)
- Rebates and refunds (28%)
- Banking (27%)
- Online shopping (24%)
- Health or medical (13%)
- Energy scams (12%)

Citizens Advice has seen a range of different cost-of-living scam tactics used by scammers. These have included emails claiming to be from the regulator Ofgem asking people to enter their bank details to get the £400 energy rebate, or claiming the government is giving £200,000 out at random to people who are of pension age, disabled or on a low income. None of these are genuine.

Things to be mindful of:

- **Beware of texts asking you to claim or apply for cost-of-living help – payments are automatic.** Department for Work and Pensions (DWP) have seen texts claiming to come from "Gov.org" and one which said it was from DWP. Some people had received scam texts followed up by an email asking them to call a fake number to provide more information.

Remember, you don't need to apply or do anything else to claim the cost of living payments. If you're eligible, you'll automatically receive the money straight into your bank account

- **Councils will NEVER call to ask for your bank details.** Several councils have urged households not to give out their bank or card details over the phone if they get a call about council tax rebates. In most cases, such rebates are paid automatically to those who pay their council tax by direct debit.
- **Ofgem is NOT offering a £400 energy rebate – so beware of scammers telling you this.** Energy regulator Ofgem has written to all domestic energy providers asking them to make customers aware of a scam text inviting people to apply for a bogus £400 rebate. You will never be texted by Ofgem to sign up for anything to get money or a rebate – so if you get a text like this, don't respond to it or click any links.

If you have been scammed:

- Talk to your bank or card company immediately if you have handed over any financial and sensitive information or made a payment.
- Report the scam to Action Fraud on 0300 123 2040 or use the Action Fraud online reporting tool using our online reporting tool.
- Text scams can be reported to your mobile phone provider by forwarding it to 7726 (SPAM)
- Beware of follow up scams. Sometimes after reporting a scam, you might get targeted again by a fraudster who says they can get your money back. Change your contact details- sadly, if you have been scammed once, you are more likely to be targeted again. It might be worth changing your number and/or email address if you are being bombarded by cold calls and spam.

If you still need further advice, contact the Citizens Advice Consumer Helpline on freephone 0808 223 1133.

Check A Website

Get Safe Online have partnered with Cifas, the UK's leading fraud prevention service, to launch a new Check a Website page. This is an easy-to-use online tool which can help you to determine whether a website is likely to be legitimate or a scam before you visit it. Users simply type in the address of the website they want to check, and their results will appear within seconds. It is expected to prevent thousands of people in the UK falling victim to unwanted online scams every year.

Hosted on Get Safe Online's UK website, you can access this new feature using the following link: https://www.getsafeonline.org/checkawebsite/

Courier Fraud

Courier fraud involves fraudsters telephoning a potential victim, claiming to be from their bank, the police, or another law enforcement authority, and tricking them into revealing their PIN number, bank card and personal details.

Courtesy: The charity Crimestoppers

How do criminals trick people into courier fraud?

- Scammers call victims pretending to be the police or their bank, knowing just enough details, like names or addresses, to sound convincing. The scam centres around there being an issue around the victim's banking, and that without the victim's co-operation they, or their money, will be at risk.
- The scammers scare victims with threats of arrest or causing problems with getting the money back if they tell anyone or won't co-operate. They may even prompt victims to call their bank or local police force so victims can check that this is a real investigation, to lure the victim into a false sense of security.
- When victims try this, they're not actually being disconnected from the original call, so whilst they think they are verifying details with someone new, they're still on the same phone call, and talking to the same group of scammers.
- The 'courier' part of courier fraud is there because scammers will send someone round to collect the 'evidence' – usually cash or bank cards complete with pin numbers – or in some cases actually pick the victims up and take them to a bank, jewellers, or currency exchange to withdraw cash or buy expensive items to use as collateral in the investigation.

Help & support for victims

Being scammed by courier fraud isn't just financially devastating; the emotional toll it can take can be incredibly difficult. However, there is always support available:

- To report if you've been a victim of a scam, Action Fraud are available to help on 0300 123 2040
- In an emergency, always call 999.
- If you've already given your bank details over the phone or handed your card to a courier, call your bank straight away.

Loan Fee Fraud

Loan fee fraud is an increasingly common scam. This has been reported by consumers who have been asked to pay a fee – usually between £25 and £450 – for a loan or credit that they then never received. This is a scam known as 'loan fee fraud' or 'advance fee fraud'.

Spot the warning signs of loan fee fraud:

- You may have made several loan applications online and then been contacted out of the blue by text, email or phone and offered a loan.
- You may be asked to make an upfront payment into a bank account, or transfer money via an unusual method.
- The scammers may claim that the fee is refundable and will be used as a deposit, administrative fee, insurance or because of bad credit history.
- You may be put under pressure to pay the fee quickly.
- Once the first payment has been made, the scammer might contact you again to ask for more payments before they can give you the loan.
- Even though you make the payments, you never receive the loan.

Protect yourself with this quick three-step check:

💸 If you're asked to pay an upfront fee, it could be a scam.
👈 If you're asked to pay quickly, it could be a scam.
🤔 If you're asked to pay in an unusual way, such as vouchers or money transfer, it could be a scam.

Always check that the provider is authorised by the FCA before you borrow.
Visit https://register.fca.org.uk/

Out & About…

Trading Standards attended the Parish Council Liaison event at County Hall in July which was an opportunity for delegates to talk to Leicestershire County Council service departments and Partner Agencies to find information, advice, and guidance on a variety of topics.

If you would like Trading Standards to attend your local event or to provide a scams awareness raising session, please email tradingstandards@leics.gov.uk

Finally,

Here's how you can report a wide variety of scams quickly

The National Cyber Security Centre (NCSC) sets out several different ways to report scams depending on the type:

- **Email scams.** If you get a dodgy looking email, you can report it to the National Cyber Security Centre (NCSC) by forwarding it to report@phishing.gov.uk. Remember not to click on any links within these emails.

- **Text scams.** If you get a suspicious text message, you can forward it to the number 7726 – this will allow your provider to track the origin of the text and arrange to block or ban the sender if it's a scam. You can also report scam text messages to report@phishing.gov.uk by providing a screenshot of the text message.

- **Website scams.** If you notice a website that doesn't look quite right, you can easily report the URL to the NCSC directly via its online form - https://www.ncsc.gov.uk/section/about-this-website/report-scam-website

- **Scam adverts.** These can currently be reported to the Advertising Standards Authority (ASA) through its online form - https://www.asa.org.uk/make-a-complaint/report-an-online-scam-ad.html

If you have been a victim of a scam or require further advice, 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