Trading Standards Scams News

A round-up of the latest scams alerts

Leicestershire County Council

Spring 2023

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 Scams

Criminals often play to people's emotions to commit fraud and at a time when many of us are anxious about money, fraudsters are grabbing the opportunity to scam people. They may pretend to be legitimate companies, such as energy providers or the government, to trick people into handing over their money or personal details. For example, with the fake offer of an energy rebate or cost-of-living payment. Then the criminals can use your details to steal your money or to commit further fraud.

Here we will look at some of the most common Cost of Living scams, so you know what to look out for. Different scams will crop up as new Cost of Living schemes are launched, but the advice is often the same: **stop and think before handing over your personal and/or financial details, clicking on a link or sending a payment.**

Energy Bill Rebates

Scammers have been taking advantage of rising energy bills by sending messages pretending to offer energy rebates. Many of these scams have capitalised on the roll out of the government's Energy Bill Support Scheme. Although this financial support will have come to an end by March 2023, look out for fraudsters attempts to scam consumers by asking for personal information to check eligibility for further financial support for example.

Criminals are experts at spoofing emails and messages, it may look as though they've come from your energy provider or the government. The messages may vary, but they may ask you to check if you're entitled to a rebate, or to register for a rebate by clicking on a link. These links then lead to genuine looking websites set up to steal personal and financial information. In some cases, scammers will then ask people to register for the payment by entering their personal information and bank details. These are then used to steal money and

comment further fraud. In some cases, they may do this by calling the victim, pretending to be their bank. They will use the personal or financial details that they've already taken to convince them of this, and to manipulate the person into handing over further details or money.

Remember: The Energy Bill Support Scheme comes to an end in March 2023 and residents will no longer receive Governments funding automatically in their energy accounts. Be suspicious of any messages asking you to register for an energy rebate or to supply your bank details.

Cost-of-living payments

The Department for Work and Pensions (DWP) has announced that cost-of-living payments will be made between Spring 2023 and Spring 2024 to help support people financially. With this, the DWP have warned of scams from criminals asking people to apply for these payments. These scams often work in a similar way to energy rebate scams, with fraudsters pretending to be the DWP or another organisation offering to help with cost-of-living payments. Again, avoid clicking on links in messages as they may take you to malicious websites designed to steal your personal information and banking details. If you're eligible for cost-of-living payments, you won't need to apply for the payment or contact the DWP directly.

Remember: Payment will be made for you automatically in the way you usually get your benefits or tax credits. Visit the correct organisations website when applying for benefits rather than clicking on a link in a message you're not sure about.

Fake vouchers, discounts and offers

Fraudsters are taking advantage of rising living costs with scams which claim to help you save money on essentials. Be cautious of deals that seem too good to be true**.** According to Action Fraud, there has been a rise in phishing emails claiming to provide savings on energy bills, as we have seen above, but also offering fuel vouchers, phone bill discounts and supermarket offers. Scams may also come in the form of spoofed adverts on social media or websites, offering deals or giveaways. These adverts may mimic well-known supermarkets and brands, but in fact lead to 'fake' websites designed to steal your personal information.

Remember: If you see an offer, don't click on the link, or the advert itself. Instead, check the brand's official website or social media to see whether the offer is authentic. And remember, if an offer seems too good to be true, it probably is.

How to protect yourself

Don't

- ! Share your bank or card details resulting from an unsolicited phone call, email, or message.
- ! Click on links or attachments included in unsolicited emails or messages.

- ! Assume that an email, phone call or text message is authentic, even they seem to know things about you.

Do

- ✓ Check email addresses, phone numbers and URLs to see if they look suspicious.
- ✓ Visit the organisations website by searching your browser rather than clicking on a link or advert.
- ✓ Call companies back using the number on their website to confirm whether a message is genuine.
- ✓ If you think you've fallen victim to a phishing scam, contact your bank straight away to report it.
- ✓ Always check by contacting the legitimate organisation using their details from a bill, letter or from the official website.

Unwanted Charity Mail

Trading Standards have been working with a Leicestershire resident who was being inundated with numerous charity and prize draw letters. Although the resident was already making regular donations, not only were they were receiving letters asking them to increase their donation amount, but also received 'begging' letters from organisations they had never had any contact with. Out of kindness and feelings of guilt, the resident was making even further donations. When this became unmanageable, he was left feeling overwhelmed and distressed. Trading Standards stepped in to assist by contacting over 90 charities to request his details be removed from their mailing lists and removing hundreds of letters from his property. We worked with the resident, taking into consideration his wishes, and stopped any unwanted donation payments being taken from his account.

Let's look at how this problem can occur and what to do about it.

How Does My Name Get on Lists?

Contributing to a charity adds your name to its "donor" list. That list can be shared with other organisations that are looking for potential donors and the result is mail from both the charity you first gave to and those with whom it shared your personal details. Generally, charities deal with list brokers who help them to identify and then access lists of names with a good potential for becoming givers. Not all names come from other charities; your name on a list of subscribers to a special-interest magazine, or among buyers of a certain product or service, for example, may end up on a list used by charities to solicit donors.

It's often difficult to know where a charity got your details from, because fundraisers may cast a wide net. For example, a charity focused on children's leukaemia, might initially seek lists not only of those who had donated to a similar charity, or shown interest in leukaemia, but

also to those who'd reacted positively to children's issues, and possibly to those who gave to cancer or even to other diseases.

If you, or someone you know is feeling overwhelmed by unwanted marketing mail from a charity or charities, here is what you can do:

- ✓ Register with the Mailing Preference Service (MPS)
  This removes your name from mailing lists, and helps you stop receiving advertising material that is personally addressed to you. It can take up to four months for the register to take effect. Register for free online or call them on 020 7291 3310.
- ✓ Contact your local electoral registration office and ask them to take your details off the 'open' register. The open register is a list of people's names and address which can be bought by companies looking to mail advertisements and promotions.
- ✓ Register with the Fundraising Preference Service (FPS). This will stop marketing mail from a charity registered in England, Wales or Northern Ireland. Registering with the website will allow you to end contact with up to 3 charities. If you prefer, you can call the FPS on 0300 3033 517, where you can end contact with up to 20 charities at a time. You will need to have the contact details and the charity name or charity registration number to hand. Or, you can visit their webpage at www.fundraisingpreference.org.uk/learn

Warranty Scams

One of the most frequently reported phone scams is the misleading sale of insurance or warranties for white goods and appliances. The aim of most warranty or insurance scam calls is to obtain your personal details and encourage you to sign up to an unnecessary contract.

Scammers may say the following:

I'm calling from your insurance company to let you know that your washing machine / oven / dishwasher / television / boiler cover is due for renewal. We can offer you a special deal if you agree to renew today.

Our records show that you need to renew your plumbing / drainage cover. We can take payment now over the phone - please confirm your contact details

You're paying too much for your appliance insurance. I can offer you a cheaper price - I'll just need you to give me your details so that I can sign you up for a monthly direct debit

How can I tell if a call about my insurance or warranty is a scam?

- Legitimate companies will never phone you unexpectedly to ask you to provide your personal or banking details.
- Be suspicious of any cold caller who asks you to share or confirm any details.
- Scam phone calls often ask you to act urgently to avoid losing money. The caller might pretend that you already have a policy with them and offer to renew it for a cheaper price. They may say that this deal is only available for a short time to try and encourage you to sign you up for monthly direct debits.
- Many common appliance issues are covered by people's existing home contents insurance, meaning that you might not even need appliance breakdown cover.

What should I do if I get one of these calls?

- If you receive a similar cold call and are not sure whether it is legitimate, hang up and contact the original supplier to check whether you need a new warranty.
- Never give a cold caller any personal information or bank details, even if they seem to know some of your details already.
- Don't agree to make any payments on the spot. Take time to think about your decision and, if in doubt, contact the original supplier of the appliance.

Arranging and providing insurance contracts is a regulated activity, which means the company offering it to you must be authorised by the Financial Conduct Authority.

Remember: if it sounds too good to be true, it probably is.

Finally....

If you would like to report a scam, or you have been a victim of 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 at: www.facebook.com/leicstradingstandards

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