Trading Standards Scams News

A round-up of the latest scams alerts

Leicestershire County Council

Summer 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.

Digital Scams

Digital (also known as cyber) scams are any type of fraud that is perpetrated online using digital devices such as a computer, tablet, or smartphone, resulting in the loss of money, personal information, or passwords for the consumer. Criminals are using social media, email, and messaging services to target potential victims, and are getting more sophisticated in how they use technology to grow their reach. But that doesn't mean anyone has to become a victim. By understanding how the fraudsters operate and knowing the key warning signs, you can avoid falling for their scams.

What techniques do scammers use to fool us?

While computer scams use technology, they tend to work using many of the same techniques as 'real-world' scams. This is known as 'social engineering' – fraudsters manipulate how people typically think and behave to get us to divulge sensitive information or hand out money or give them access to computers or data. For instance, you might get fraudulent emails claiming to come from your bank, which direct you to a website where you'll enter your online banking credentials. Or you might get a call from someone offering to fix a security problem on your computer when they really want you to install software they can use to steal your most sensitive data. Scammers will pretend that they're protecting you, or doing you a favour, and even promise amazing offers that will save you money. All the time, they're trying to pressure you into doing what they want. Often, they will apply time pressure; act quickly to stay safe, avoid missing out on a good deal etc.

What are scammers looking for?

Most scams are financially motivated, many though, are aimed at extracting information for financial gain, looking for any credentials you use when logging onto online banking or shopping with a credit card, or any information they can use to access your email or any online accounts. However, it's not just the obvious signs that should concern you. Even a seeming harmless quiz on social media can be used to get information – like your first pet, your first school or your date of birth – that could be used elsewhere to answer, say, a security question protecting your online banking.

3. How might fraudsters approach us?

The main techniques the fraudsters use doesn't change that much, the scams themselves keep evolving. Sometimes scams are recurring so you may see emails from the HMRC appearing at the end of the tax year, or parcel delivery scams in the run-up to Christmas, Black Friday sales have also become a focal point for fraudsters operating fake online stores. In other cases, scammers take advantage of real-world events. The Covid-19 pandemic inspired a wave of fake emails, text messages and phone calls appearing to come from the government, the NHS, HMRC or the Track and Trace programme. Other scams are just a case of the scammer trying something that they hope will affect a wide group of people, which is why so many use the TV license, BT Broadband services, or a problem with your laptop. You might even get messages about renewing an Amazon Prime account. The scammers don't actually know whether you use the products or services mentioned, but they know that enough people do that it's worth a try.

4. Why is this scam targeting me?

These scams aren't personal, and they're usually designed to work across a wide range of people in the hope that even a few of us will get caught out. However, some people are more vulnerable than others, and scammers love to prey on older people who may be lonely or less confident with technology, or who may have age-related conditions.

They will work hard to confuse and apply pressure to people who might not immediately spot the scam, or who might need support and advice before they say 'no.'

The best weapon against them is to pause and take stock, as outlined by the campaign **Take Five**. Stop and ask yourself:

- Have you been contacted out of the blue?
- Have you been asked to share personal details – especially unnecessary details?
- Are you being asked to install software or provide access to a computer, phone or tablet, or an online service or account?
- Does the person you are dealing with have all the information that a real representative of a company or organization would?

- Are they asking you to do something urgently or not mention what's happening to your friends, your family, or your bank?

If something seems suspicious, it probably is, so don't get pressured into moving forward. For more detailed information about online banking and shopping, there are some great resources
at https://getsafeonline.org/ and https://www.moneyadviceservice.org.uk/en/articles/beginners-guide-to-online-banking.

Summer Rogue Trader Warning

Be wary of cold callers or leaflets offering to undertake garden clearances, tree cutting and work to roofs and gutters, or even home improvements. Citizens Advice are encouraging caution if anyone knocks on your door and offers to start work immediately, particularly if they are pushy or claim that urgent repairs are needed.

The warning comes in conjunction with scams awareness week campaign which runs from 3 – 9 July, but it's important to be scam aware all year round.

Rogue traders will target residents who may be elderly or vulnerable and overcharge for doing very little work. In some instances, leave the victim having to find a reputable trader to put right what they have done. They defraud victims through pressure selling, often offering substantial reductions to start the work there and then, breaching the victim's legal rights of a cooling off period. They then escalate the price once work has started. After carrying out work such as cutting back trees, they may charge to take the waste away and then often dump it illegally. While cold calling is not against the law, it may be that the trader isn't all they seem and may be committing a criminal offence.

Trading Standards advice if you need work carrying out:

- ✓ Get at least three quotes from traders known to you, family, or friends
- ✓ Do not answer the door to traders you do not know or have not asked to visit
- ✓ Display a no cold calling notice deter cold callers (You can request one from Trading Standards using the contact details at the end of this newsletter)
- ✓ You can report cold callers to Citizens Advice consumer helpline on **0808 223 1133**

IT'S A SCAM

Fraudsters are pretending to be police officers to get your cash!

1 THE PHONE CALL

A fraudster telephones you claiming to be a police officer. They tell you that the money in your bank might include counterfeit notes.

2 YOUR CASH

They ask you to withdraw £5,000 (or more) in cash from your bank account so they can collect it in order to investigate.

3 THE COURIER

They will send a taxi with a courier to collect your cash.

JUST REMEMBER:

Your bank or the police would never ask you to hand over cash, bank cards or your PIN. Don't give them to anybody!

leics.police.uk

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

Leicestershire Police
Protecting our communities

Out & About

Our Trading Standards Scams Officer went out to deliver a scams awareness session to the members Hinckley U3A. They were a fantastic group of local residents who were very engaging by sharing experiences and having conversations around keeping safe from scams. This helps to break down the stigma of being a scam victim and encourages people to have conversations around this issue.

We highlighted the latest scams, talked about keeping yourself safe, and reminded people to be vigilant and also to look out for our family, friends and neighbours.

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

Parcel Delivery Fraud

Parcel Delivery scams are by far the most common scam faced by consumers this year according to new research by the Citizens Advice, released as part to the Scams Awareness Campaign 2023. Almost half of people (49%) targeted by scammers had been on the receiving end of a malicious parcel delivery scam, with fraudsters attempting to get hold of personal information or bank details. The charity's research also reveals that 40 million people have been targeted by scams already in 2023.

If you're expecting a delivery and you receive a 'missed parcel' message:

1. Do **not** click the link and never give out personal bank details.
2. Use the **official websites** of delivery companies to track your parcel.
3. Forward the message to **7726**, a free spam-reporting service provided by phone operators. If you are not sure how to forward a text message from your particular device, search online for instructions.
4. **Delete** the message.

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

Fraud is a serious issue in the UK, with consumers' losing over £1.2bn in 2022, the equivalent to £2,300 every minute, states an Annual Fraud Report by UK Finance.

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