Trading Standards Scams News

A round-up of the latest scams alerts

Leicestershire County Council

Autumn 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.

Black Friday/Cyber Monday Scams

Black Friday is an annual sales event which takes place on November 24, 2023, although many of the reduced prices will continue to be available until Cyber Monday, on November 27, 2023. These yearly shopping events are a prime time for scammers to try and take advantage of unsuspecting shoppers. To protect yourself and your financial information, it's important to be aware of online scams and only shop from reputable websites during the Black Friday/Cyber Monday period. Here are some tips to help you do just that:

- ✓ **Stick to well-known and trusted retailers -** These retailers typically have strong security measures in place to protect your personal and financial information.
- ✓ **Check the web address -** Before entering any personal or financial information, check the website address, also known as a URL, to make sure it's legitimate. If it looks unusual or has typos in it, it’s likely a scam. Fraudsters create fake websites that look like real ones in order to trick people into entering their information.
- ✓ **Look for the padlock symbol -** Check to make sure the website you're shopping on has a padlock symbol in the website address bar. This means that the site is encrypted, which means your information will be protected.
- ✓ **Avoid clicking on links in emails -** Be wary of emails that offer amazing deals or discounts, especially if they include a link to a website. Scammers will often send out what’s called a ‘phishing’ email that look like they're from a legitimate retailer in an attempt to steal your information.
- ✓ **Use strong passwords -** Make sure you're using strong passwords that are difficult to guess. Create unique passwords for each online shopping account you have and avoid using easy-to-guess passwords such as "123456" or "password." Also, avoid

using the same password for multiple accounts, and consider using a password manager to keep your passwords organized and secure.

- ✓ **Use a secure payment method -** When shopping online, use a secure payment method such as a credit card or PayPal. These methods offer added protection in case of fraud or unauthorised charges.

If something seems suspicious, it probably is. For more detailed information about online shopping and banking safely, there are some great resources at **Get safe online** and **Money advice service - beginners-guide-to-online-banking**.

! Be Scam Aware !

If you receive an unexpected call from someone claiming to be from an organisation, such as your local council or you bank, and they are asking for personal or sensitive information, remember, you do not have to provide it to them.

If you are concerned, hang up the phone and call the organisation back on a genuine, trusted number.

Watch out for Recovery Fraud

Also known as recovery/refund scams - this type of scam allows criminals to target people who have already lost money to a scam. Typically, recent victims of bank transfer scams and investment scams are targeted, but criminals will target anyone if it's known to them that you have responded to some type of scam. So, if you've recently fallen victim, be on your guard against fraudsters contacting you to claim they can get your money back. Read on to find out more about how recovery scams work and for advice on staying safe if you've been scammed.

The most common tactics used in recovery scams include fraudsters contacting you out of the blue and pressuring you to use their 'service', requesting your bank details and asking for an upfront fee. In some instances, they will create professional-looking websites with fake five-star reviews to make things seem legitimate.

Alternatively, you may come across recovery scammers on social media, stalking platforms in search of victims, and even impersonating ombudsmen and regulators to convince victims they're genuine.

Keep an eye out for suspected scammers which operate on both Facebook and X (formerly known as Twitter), reaching out to people who have posted that they'd been scammed, again, by claiming to offer recovery services and charging an upfront fee.

How to avoid recovery scams

If you've been scammed, it's vital to be on your guard against any calls, texts, emails and social media messages from people claiming they can get your money back. If anyone asks you to pay a fee or provide your bank account or card details, end all contact immediately.

Getting your money back after a scam

- ✓ If you've been scammed, call your bank straight away using the number on the back of your card or your bank statement.
- ✓ You should also report the scam to Action Fraud and Citizen's Advice Consumer Service – contact details at the bottom of this newsletter.
- ✓ You can ask your bank to reimburse your losses. Many banks are signed up to a code designed to protect innocent victims of fraud. If your bank rejects your claim, you can escalate the case to the Financial Ombudsman.
- ✓ None of these steps will cost you money, and although there may be paid services out there, you don't need to enlist the services of a third party to help you make a claim.

How to report dodgy accounts and websites

You can report Facebook accounts, groups and posts by tapping the three dots in the top right-hand corner of the page and selecting 'report.'

To report an account on X, tap the three dots above its bio and select 'report.' You can report individual posts by tapping the three dots above the posts and selecting 'report.'

Suspicious websites should be reported to the National Cyber Security Centre.

TS Facebook

Did you know Trading Standards have their own Facebook page? Keep up to date with the latest scams alerts and other warnings that we put out to help keep residents safe. Go to www.facebook.com/leicstradingstandards and click 'Follow'.

A warning to landline users

The Local Government Association (LGA) has warned that criminals are exploiting the upcoming digital switchover and has urged people to be aware of potential scams.

Fraudsters are taking advantage of the analogue to digital switchover in the UK's telephone network to scam elderly and vulnerable people. The changeover will see most UK telephone providers move their customers from old analogue landlines to new, upgraded services which use the internet (also known as broadband), with the changes taking place up to 2025. If you already have an internet connection, then the new digital landline system will use this. If you don't, your provider will supply one specifically to support the new digital system, but you shouldn't pay extra for this if you don't move over to a broadband service.

The LGA says people who use healthcare telephone-based devices such as lifelines or personal alarms are particularly at risk of being targeted by scammers, who trick victims into disclosing their personal and financial information over the phone by claiming the resident needs to hand over bank details as part of the switchover, or they will be disconnected. Around 1.8 million people use these devices across the country, and the advice is that councils and their homecare alarm providers or contractors will never ask for personal or financial information over the phone. Please remember - the switchover is free of charge and will be straightforward for most people. Scam attempts are expected to increase as the switchover date nears, and in addition to phone calls, criminals may create phishing emails and fake websites to get your personal data.

Reporting nuisance calls

- ✓ Scam phone calls can be reported by texting the word ‘call’ and the scam phone number to 7726.
- ✓ You can report scam callers on WhatsApp by tapping 'report contact' and 'block' after opening up the chat with the dodgy phone number.
- ✓ Suspicious emails should be forwarded to report@phishing.gov.uk, and scam websites can be reported to the NCSC online.
- ✓ You can also report scams to Action Fraud online or by calling 0300 123 2040.

Trader schemes used by Rogue traders

Rogue traders are taking advantage of trade organisation schemes online, whereby they are advertising to be reputable trades people. Just because a trader is advertising on a trade organisation site, it doesn’t mean that they are legitimate. Rogue traders have been using them to appear genuine.

Recently, a resident within the Leicestershire area was defrauded of their whole life savings by a rogue trader who implied they were carrying out pest control, roofing, and gardening works. They even offered investment opportunities to the victim, this never materialised, and works were never carried out.

Rogue traders like this are experts at extorting monies out of people. They can often befriend you at first but can then use aggressive practices when they don’t get what they want. Eventually they can be emotionally and mentally abusive, and they will go to great lengths to get money out of you. When something seems too good to be true, it often is.

If you feel that you have been a victim of a scam, contact your bank to see if they can offer any further assistance. Please be aware that Trading Standards cannot get your money back for you, but when a report like this is received, any action is taken in-line with our enforcement policy. In an emergency, or if you feel threatened or intimidated, please call 999. For further free advice, and guidance or to a report a matter, please contact 0808 223 11

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 – www.actionfraud.police.uk or call 0300 123 2040

Citizens Advice Consumer Helpline - 0808 223 1133

You can find consumer education resources at: www.citizensadvice.org.uk

You can request scams leaflets and door stickers from Leicestershire County Council at: www.leicestershire.gov.uk

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