Trading Standards Scams News

A round-up of the latest scams alerts

Leicestershire County Council

AUTUMN 2026

Welcome to our Scams Newsletter

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.

Courier Fraud Warning

🚨 Don't Be Pressured into Handing Over Your Money

Courier fraud is a sophisticated scam that continues to target people across the UK, often causing significant financial and emotional harm. Criminals are skilled at convincing victims that they are speaking to trusted organisations such as their bank, the police, or government agencies.



The scam usually begins with an unexpected phone call. The caller may claim that your bank account has been compromised or that counterfeit money has been detected in your area. Sometimes they pretend to be a police officer investigating fraud and ask for your help with a supposed investigation.

To gain your trust, the fraudster may know personal information about you and may pressure you into acting quickly. Victims are often instructed to withdraw cash, purchase expensive items, or gift cards, or disclose banking information. A courier is then sent to collect the money, cards, or valuables from the victim's home.

Warning Signs

Be suspicious if someone:



🚩 Claims to be from your bank, the police, or another trusted organisation and asks you to keep the call confidential.

🚩 Tells you there is an urgent problem with your bank account.

🚩 Asks you to withdraw cash or transfer money to a "safe account".

🚩 Requests your PIN, online banking passwords, or one-time security codes.

🚩 Arranges for a courier to collect cash, bank cards, jewellery, or other valuables from your home.

🚩 Pressures you to act immediately without seeking independent advice.

Protect Yourself

Remember these important points:

✅ Your bank will never ask you to withdraw cash or transfer money to a safe account.

✅ The police will never ask you to assist an investigation by withdrawing money or handing over valuables.

✅ Never reveal your PIN, passwords, or security codes to anyone.

✅ If you receive an unexpected call, hang up and use a different phone or wait at least five minutes before calling the organisation back using a number you trust.

✅ Talk to a family member, friend, or neighbour before making financial decisions under pressure.

If You Think You Have Been Targeted

If you believe you have been contacted by a courier fraudster:

🚫 End the call immediately.

🏦 Contact your bank using the number on the back of your card.

☎️ Report the incident to Report Fraud on 0300 123 2040 or via www.reportfraud.police.uk

🚨 If a crime is in progress or you feel threatened, call 999.

Help Protect Others

Courier fraudsters often target older and more vulnerable members of our communities. By talking openly about scams with friends, relatives, and neighbours, we can help prevent others from becoming victims.

Remember: **If someone contacts you unexpectedly and asks for money, bank details, or valuables, stop, think, and verify before you act.** A genuine organisation will never object to you taking time to check who they are.

Raising Cybercrime Awareness

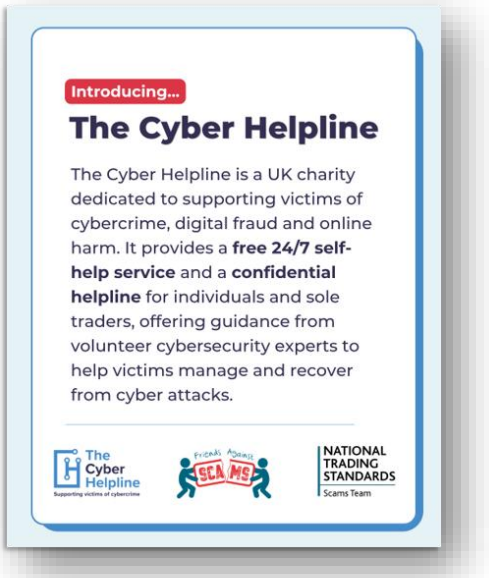
🚨 What You Need to Know

What Is Cybercrime?

Cybercrime is any illegal activity carried out online or using digital devices such as computers, smartphones, and tablets.

Criminals can use technology to target individuals, commit offences, or facilitate other criminal activity.

Common examples include hacking, ransomware, fraud, identity theft, online harassment, and cyberstalking. With more of everyday life taking place online, cybercrime continues to present a significant challenge.



In 2025, 58% of crimes in England and Wales were online or cyber-enabled, affecting over 5 million victims.

Who Is at Risk?

Cybercrime can happen to anyone. Criminals use increasingly convincing tactics designed to gain trust, create pressure, and make their approach appear genuine.

Some people may be particularly vulnerable, including older adults and those facing emotional or financial challenges. Being targeted is not the victim's fault. Removing stigma is important so that people feel able to speak up, report incidents and seek support.

Common Enablers of Cybercrime

Cybercriminals often take advantage of everyday behaviours and security weaknesses. Understanding these common risk factors can help people stay safer online.

🔐 **Weak security –** Weak or reused passwords and no two-factor authentication.

🔄 **Outdated software –** Missed updates can leave devices vulnerable**.**

🔗 **Suspicious links –** Can lead to phishing or malware.

🧩 **Oversharing online –** Personal details can help criminals target you.

💬 **Unexpected contact –** Unsolicited messages can catch you off guard.



⏰ **Pressure tactics –** Urgency or emotion can lead to rushed decisions.

🤝 **Misplaced trust –** Criminals may build trust to obtain sensitive information.

💞 **Relationships** – Personal connections can be exploited.

💷 **Investment offers –** Promises of quick returns can be a warning sign.

🛡️ **Lack of awareness –** Knowing the warning signs can help keep you safe.

Stop and think before clicking links, sharing information, or sending money. If something does not feel right, take time to check it independently.

Stay Safe Online This Black Friday and Christmas

🚨 A Warning for Bargain Hunters

While the festive period offers fantastic opportunities to save money, it is also one of the busiest times of year for fraudsters, who are quick to exploit shoppers looking for deals.

By taking a few simple precautions, you can help protect yourself and your finances while enjoying your festive shopping.



Watch Out for Fake Deals

Scammers often create convincing websites, social media adverts and emails promoting heavily discounted products. If a deal seems too good to be true, it probably is.

Before making a purchase:

🛍️ **Research the retailer** and look for genuine customer reviews.

🔎 **Check the website address** is legitimate and correctly spelt.

💷 **Be wary of low prices** on new or unfamiliar websites.

🔗 **Avoid unsolicited links** in emails, texts, or social media messages.

Pay Securely

Using secure payment methods provides additional protection if something goes wrong.

Consider the following:

💳 **Pay by credit card where possible**, particularly for higher-value purchases.

🔒 **Use reputable payment services**, such as PayPal or other recognised digital wallets.

⚠️ **Be cautious about paying by bank transfer** when dealing with an unfamiliar seller, as recovering your money may be more difficult if something goes wrong.

Protect Your Personal Information

Fraudsters often use shopping scams to steal personal and financial information.

To stay safe:

🔑 **Never share passwords** or one-time security codes with anyone.

💪 **Use strong, unique passwords** for each online account.

🔐 **Enable extra security** by using multi-factor authentication wherever available**.**

🛒 **Limit personal information** by only providing what is necessary to complete your purchase.

Beware of Phishing Messages

During the festive season, scammers send fake emails and text messages claiming to be from retailers, delivery companies, or banks.

Common tactics include:

📦 Fake parcel delivery notifications.

💳 Requests to update payment details.

⚠️ Alerts claiming there is a problem with your order.

If you receive an unexpected message, do not click links or open attachments. Instead, visit the retailer's official website directly or contact the company using trusted contact details.

Shop on Secure Connections

Avoid making purchases when connected to public Wi-Fi networks in cafés, shopping centres, or transport hubs.

When shopping online:

- 🛜 Use your home internet connection or a trusted mobile network.
- 🔒 Ensure websites use secure connections, indicated by "https://" and a padlock symbol in the browser address bar.
- 💻 Keep your devices, browsers, and security software up to date.

Check Your Bank Statements

Regularly review your bank and credit card statements, especially after making online purchases.

Look out for:



- ❓ Unrecognised transactions
- 💸 Small test payments you do not recognise.
- 💷 Multiple payments to unfamiliar retailers.
- 🚩 Report suspicious activity to your bank immediately.

Take Your Time

Scammers often create a sense of urgency, claiming that offers are about to expire or that stock is running out.

Remember:

- ⏳ Genuine retailers rarely pressure customers into making immediate decisions.
- 🔍 Take time to verify retailers and offers before parting with your money.
- 🛡️ A few minutes of checking could save you from losing money and personal information.

Final Thought

Black Friday and Christmas are exciting times for shoppers, but they are also peak times for fraud. Staying alert, using secure payment methods and being cautious of unexpected messages can help ensure your festive shopping remains safe, enjoyable, and scam-free.

Think before you click, check before you buy, and enjoy a safer festive shopping season.



Finally….

⚙️Useful tools and resources:

- Check if something might be a scam here:

👉🏻 www.citizensadvice.org.uk/consumer/scams/check-if-something-might-be-a-scam

- Check if a telephone number might be a scam here 👉🏻 www.who-called.co.uk

📞 If you would like to report a scam, or you have been a victim of fraud, you can get in touch with the following organisations:

- Report Fraud – www.reportfraud.police.uk or call on 0300 123 2040 to report fraud and cyber-crime.

- Citizens Advice Consumer Helpline - 0808 223 1133 for further advice and next steps.

- If you think fraudsters may have obtained your money, contact your bank immediately using the contact details on the back of your card or bank statement.

- To keep up to date with the latest scams advice & information, you can join over 3000 followers on the Leicestershire Trading Standards Service Facebook page here 👉🏻 www.facebook.com/leicstradingstandards



Leicestershire Trading Standards Service
Email: tradingstandards@leics.gov.uk **Facebook**/LeicsTradingStandards

STOP! THINK FRAUD
NATIONAL CAMPAIGN AGAINST FRAUD
Find out how to stay ahead of scams at gov.uk/stopthinkfraud >>
UK Government