# Trading Standards Scams News

A round-up of the latest scams alerts

Leicestershire County Council

**Autumn 2025**

## 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.

---

# Pension Fraud Warning

### 🚨 Warning: Pension Fraud on the Rise – £17.5M Lost in 2024

As pension fraud continues to rise across the UK, authorities are urging savers, especially those nearing retirement, to stay vigilant against increasingly sophisticated scams.

In 2024 alone, over £17.5 million was lost to pension fraud, with victims losing an average of £33,848.


### 🔍 How are scammers targeting pension holders?

❌ Impersonation Scams:
Fraudsters hack email accounts or gather personal data to impersonate pension holders and redirect funds to fake accounts.

❌ High-Pressure Investment Fraud:
Victims are pressured into transferring pensions into high-risk or fake schemes with promises of guaranteed returns or tax-free cash.

❌Early Access Scams:
Offers to “unlock” pensions before age 55 are illegal and often result in heavy tax penalties and total loss of funds.

🛡️ **How to protect yourself:**

✅ **Secure your pension account**

- Use a unique password (three random words is a good method)
- Enable 2-step verification (adds a second layer of security to your account by requiring a password and a second, unique verification method to log in)

🚫 **Ignore unsolicited offers**

- Reject any offers if you are contacted out of the blue
- Cold calling about pensions is illegal and likely a sign of a scam
- Always seek independent financial advice before making changes to your pension arrangements (check credentials, use the Financial Conduct Authority register to verify financial advisers)

⚠️ **Be cautious of investment offers**

Watch for red flags like:

- Pressure to act quickly
- Promises of guaranteed high returns
- Downplaying of the risks of losing your money

📢 **If you're targeted or think you've been scammed:**

- Report it to **Action Fraud**: actionfraud.police.uk or call **0300 123 2040**
- Contact your bank or pension provider immediately
- Monitor your accounts for suspicious activity

🔗 Learn more: https://stopthinkfraud.campaign.gov.uk/

---

# Black Friday Scams

## Black Friday and Cyber Monday 2025: Stay Safe While Shopping Online

Black Friday, traditionally held on the last Friday of November, marks the start of the festive shopping season. While it originated in the United States, it has become a major retail event in the UK. This year, Black Friday falls on 28th November, followed by Cyber Monday on 1st December, which focuses on online deals.


Unfortunately, these high-traffic shopping days also present opportunities for scammers. Cybercriminals often create fake websites, send phishing emails, and post fraudulent ads on social media to steal personal and financial information. Their aim is to harvest data such as credit card numbers, passwords, or even full identities, often for resale or unauthorised use.

With the growth of online shopping and digital payments, it's more important than ever to stay vigilant.

🔒 **Top 5 Tips to Avoid Black Friday and Cyber Monday Scams:**

1️⃣ **Stick to trusted retailers** - Shop with reputable brands that use secure payment systems and have established customer protections

2️⃣ **Be wary of unrealistic deals** - If an offer seems too good to be true, it probably is. Scammers use deep discounts to lure victims into clicking malicious links or making hasty purchases.

3️⃣ **Use secure payment methods** - Opt for credit cards or digital wallets (e.g., PayPal, Apple Pay), which offer better fraud protection when making payments.

4️⃣ **Check for website security** - Look for the padlock icon in the browser and ensure the URL (website address) begins with https:// before entering any personal or payment details.

5️⃣ **Watch out for phishing emails** - Avoid clicking on links in unsolicited emails or messages. Instead, go directly to the retailer's official website to verify any offers.

✅ You can get more advice on https://www.getsafeonline.org/

🔍 Use their website checker to spot scams before you shop!

---

# WhatsApp Scams

## 🚨 Latest WhatsApp Scams in the UK 🚨

WhatsApp scams are on the rise, targeting users with messages that appear to be from trusted contacts, businesses, or even family members. These scams often aim to steal personal information, money, or access to your account.

**Common Types of WhatsApp Scams:**

🔹 👨‍👩‍👧 **Family Impersonation**
Scammers pretend to be a family member (often a child) who's lost their phone and urgently needs money.

🔹 📲 **WhatsApp Account Takeover**
You're tricked into sharing a one-time passcode for a fake video call — which actually gives scammers control of your account.

🔹 💼 **Fake Job Offers**
Messages about amazing job opportunities lead to requests for personal info used in fraudulent loan applications.

🔹 👥 **Impersonating Group Members**
Scammers join large community or religious groups, then message members pretending to be someone trustworthy.

🔹 💰 **Fake Compensation Claims**
Scammers impersonate organisations like the Financial Services Compensation Scheme saying you're owed money — but ask for upfront payments or screen-sharing.

🔹 💘 **Romance scams**
Pretending to be interested in a relationship, then asking for money.

## 🛡️ How to Protect Yourself 🛡️

### ⚠️ Look Out for These Warning Signs

- ❌ Spelling or grammar mistakes.
- 🔗 Messages asking you to click links or download files.
- 🏦 Requests for personal info like bank details or passwords.
- 📩 Messages asking you to forward them.
- 💸 Claims you must pay to use WhatsApp (it's always free).
- 🕵️ Someone pretending to be a loved one but acting oddly.
- 🤑 Messages about winning money, jobs, or investments.
- 🤝 Someone trying to befriend you, then asking for money.

### ✅ What Should You Do?

- 🚫 Don't click suspicious links or open unknown files.
- 🔒 Don't share personal or financial info with strangers.
- 📵 Don't forward suspicious messages.
- 🧠 Ask a trusted friend or family member if unsure.
- 🚷 Block or report senders who make you uncomfortable.
- 🗑️ Delete suspicious messages.

### 🧠 Remember

- 🆓 WhatsApp is always free.
- ❗ Unbelievable deals often come with hidden surprises—stay alert
- 🗣️ If you're unsure, ask someone you trust.

🔗 For more info, visit the official WhatsApp page: **WhatsApp Suspicious Messages FAQ**

# 🚨 SCAM ALERT: Ofcom Impersonation 🚨

Scammers are impersonating Ofcom to steal personal and financial information. Stay alert and protect yourself.

## ⚠️ Scam Summary

- They falsely claim services have been fraudulently taken out in your name.
- They may pretend to transfer you to the police.
- They spoof legitimate Ofcom phone numbers:

📞 020 7981 3040
📞 020 7981 3000
📞 0300 123 3333

## 🚫 What to Do If You Receive Such a Call

❌ Do NOT share any personal or financial information.
📴 Hang up immediately.
🕵️ Report the incident to Action Fraud.

## 🔒 Ofcom's Response Measures

🚫 Blocking scam numbers using the Do Not Originate (DNO) list.
🌍 Preventing spoofed UK numbers from being used abroad.
🔍 Tightening checks on how phone numbers are allocated.

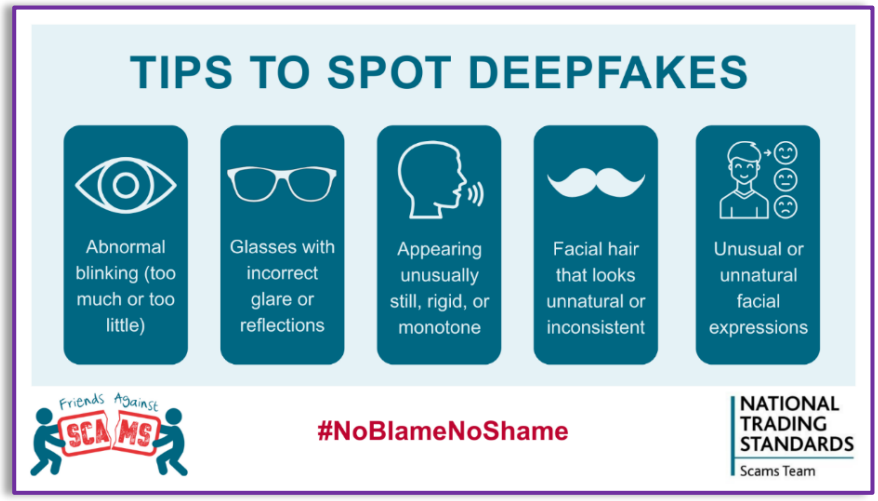
## 🔗 Where to Get More Information

🌐 Visit: https://www.ofcom.org.uk
🌐 Visit: https://stopthinkfraud.campaign.gov.uk

---

# What is a Deepfake?

Deepfakes are created by using artificial intelligence (AI) to manipulate existing footage or audio to make someone appear to say or do something they never did.




💡 Here are four common deepfake scams to be on the lookout for:

1️⃣ Investment Scams: Fake videos of public figures like Martin Lewis promoting "can't-miss" investment deals.
2️⃣ Romance Scams: AI-created profiles build fake relationships online, then ask for money.
3️⃣ Extortion Scams: Criminals use voice cloning to pretend to be a family member in trouble, urgently asking for money.
4️⃣ Celebrity Ad Scams: Fake ads using public figures to sell products they never endorsed.

🌓 Learn how to protect yourself by becoming a Friend Against Scams www.friendsagainstscams.org.uk/online-awareness-training-video #NoBlameNoShame

---

# 🎄 Stay Scam-Safe This Christmas 🎄

Christmas is a time for joy, connection, and giving—but sadly, it's also a time when fraudsters try to take advantage of people. Whether it's through phone calls, emails, or doorstep visits, criminals use clever tricks to catch people off guard.

Here are some simple ways to protect yourself and enjoy a safe, scam-free Christmas:

### 🛍️ Shopping Safely Online

Online shopping is convenient, but it's important to be cautious:

- **Use websites you know and trust**—look for the padlock symbol in the address bar.
- **Avoid clicking on links in emails or texts** unless you're sure they're genuine.
- **Be wary of "too good to be true" offers**—they often are.

If you're unsure, ask a family member or friend to help check the website before you buy.

### 📦 Fake Delivery Messages

Scammers often send texts or emails pretending to be from Royal Mail or courier companies, saying you need to pay a fee or click a link.

- **Don’t click on any links**—go directly to the company’s official website.
- **Ignore messages that feel rushed or threatening**.

If in doubt, speak to someone you trust before responding.

### 🎁 Gift Card Scams

Gift cards are popular presents, but scammers use them to steal money.

- **Never pay bills or fines with gift cards**—no real company or government office will ask you to do this.
- **Only buy gift cards from well-known shops**, and avoid offers from strangers online.

### 💔 Charity Scams

Christmas is a time for giving, but make sure your donations go to real charities.

- **Check the charity’s name on the Charity Commission website**: www.gov.uk/checkcharity
- **Don’t feel pressured to donate immediately**, especially if someone calls or knocks on your door.

Real charities will understand if you want time to think.

### 🛡️ General Tips to Stay Safe

- **Don’t share personal details** like your bank account or passwords over the phone or online.
- **Hang up on suspicious calls**—you can always call the company back using a trusted number.
- **Talk to someone you trust** if something doesn’t feel right.

### 📞 Need Help or Want to Report a Scam?

You’re not alone. If you think you’ve been targeted by a scam, contact:

- **Action Fraud**: 0300 123 2040 or www.actionfraud.police.uk
- **Citizens Advice Consumer Helpline**: 0808 223 1133

**Let’s keep the festive season full of joy - not worry. Stay alert and trust your instincts**

# Finally….

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:

Action Fraud – https://www.actionfraud.police.uk/

Citizens Advice Consumer Helpline - 0808 223 1133

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

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**

Email: tradingstandards@leics.gov.uk **Facebook** /LeicsTradingStandards