# Trading Standards Scams News

A round-up of the latest scams alerts

Leicestershire County Council

**December 2021**

## Welcome….

to the extra Christmas edition of the Leicestershire Trading Standards Service scams newsletter. With the festive season upon us, fraudsters will be working overtime this Christmas. Get the warning bells ringing by reading our round up of the 12 scams of Christmas…..

## 1. WhatsApp Scams


Fraudsters are posing as family members on WhatsApp to manipulate victims into transferring money. We have received reports of messages purporting to be from sons or daughters, addressed to 'Mum' or 'Dad' and claiming their phone has been lost or damaged and this was their new phone number. Messages will continue by saying that they have an unexpected bill that they needed money for. Once the victim has given their bank account details and the money was transferred, the victims never heard from them again. The message is to **Stop** – take time before you respond. **Think** – does this request seem genuine? Are they asking for money? **Call** – Verify the request by calling your family member to make sure it was them.

## 2. Online Shopping Scams


It can be difficult to spot a fake, fraudulent or scam website. Fraudsters are extremely cunning, using the latest technology to set up convincing websites that look like genuine online retailers. These websites will offer items such as clothing, games consoles and other desirable goods at extremely low prices to quickly sell counterfeit, or non-existent items. Our advice is – if it's too good to be true, it probably is! Choose carefully where you shop and research retailers online to make sure they're legitimate. Ensure the website is secure by looking for a

padlock next to a website's URL, this means the site is encrypted. So, what you do on it – such as browse or make payments – can't be intercepted. Secure websites begin with https:// and using a credit card if you have one, will provide some level of protection if things go wrong. Never pay for goods by bank transfer.

## 3. Phishing Emails/Texts

Phishing emails and texts don't stop over the holidays. Ignore messages claiming to be from a financial institution, telecommunications company or delivery company asking you to confirm personal information and don't click on malicious links. Fraudsters send you a message and attempt to make you click on a link to a fake site or open an attachment that infects your device with a virus. Logos, email addresses, even the link might look genuine, but you'll get more than you bargained for if you do as the email asks. They will make you panic and rush your decision.

## 4. Identity Theft and Fraud

Identity theft happens when fraudsters access enough information about someone's identity to commit identity fraud. Identity theft can take place whether the fraud victim is alive or deceased.
If you're a victim of identity theft, it can lead to fraud that can have a direct impact on your personal finances and could also make it difficult for you to obtain loans, credit cards or a mortgage until the matter is resolved. Keep your personal information safe and think twice about who you may be providing your details to. Keep wallets close, cover PINs and don't share passwords or personal information.

## 5. Social Media Scams


The scammers create social media accounts and pay to have their scam message advertised to you in your timeline. Stay vigilant when you see new companies, organisations or brands pop up on your feed. You should also be suspicious if you see a new social media account advertising for a company you know well. It may be a scammer pretending to be a new branch or new account for that brand. Also beware of free prize draw offers and giveaways as these scams rely on you to fill in your personal details to enter or claim fake prizes. Always check for legitimate terms and conditions for the giveaway and never pay to claim a prize or for postage.
Also, is what you share on social media really necessary? Could it be helping a fraudster, or telling a burglar you're away? Think before you post and take some time over Christmas to review your device and app privacy settings.

## 6. Bogus Charities

Watch out for criminals using a legitimate charity's name and appealing on their behalf, for a donation. If suspicious, ask to see their official charity ID which they're required to carry. TRUST your instincts! Fraudsters are all too ready to take advantage of the feeling of Christmas goodwill. If you receive a marketing email, check it is genuine. Check the header or hover your mouse over the link - it should read along the lines of www.charityname.com/donate. If it does not it is probably a scam.

---

## 7. Christmas Delivery Scams

The chances are that you may have done some online shopping as Christmas is fast approaching and the scammers are well aware that many of us are shopping in this way. There are different versions of this scam, but you may receive an email or text message letting you know that you are due to receive a parcel, or that you have missed a delivery. This will prompt you to click on a link and enter personal or financial details. Stop and think! Firstly, are you expecting a parcel? If so, you do not need to provide sensitive information and none of the well-known delivery companies will ask for this. If they are requesting money or personal information, alarm bells should be ringing. If you are still unsure, check with the retailer that you have placed an order with by contacting them directly.

---

## 8. Gift Card Scams


Received an email from a friend asking to buy gift cards for them? Criminals clone and pretend to be people you know to ask you to do this. They are after the code on the card to spend the money. DON'T do it. Another version of this scam is where the victim receives a call demanding an urgent payment by purchasing iTunes or other gift cards/vouchers from the nearest retailer, which could be their local shop or supermarket. The victim is told that this is to settle an overdue tax bill (fraudsters frequently claim to be representing HMRC), hospital bill, utility bill, debt collection fee or bail money. In reality, this type of gift card/voucher can be used only to purchase goods or services on the website of the business issuing it.

---

## 9. Computer Support Scams

This type of scam could be via a phone call or email claiming that they have kindly detected an error or security risk on your computer they'd like to help you fix. They will try to direct you to a bogus website. Companies like Microsoft will NEVER call you directly. The scammer then asks for permission to remote into your computer. They may ask you to download special software to enable this. Next, they may show you "log files", which are normal but claim these are bugs that need fixing. They will then ask for credit card details to charge you to fix them - or convince you to subscribe to a service that supports you.

---

## 10. Supermarket Voucher Scams

Planning to cook a family feast this Christmas? Scammers have sent out a raft of emails claiming to be offering FREE vouchers at major supermarkets. Fake vouchers are circulating claiming to come from the likes of Aldi, Lidl, Tesco and Waitrose. Scammers are distributing them via a variety of channels, including email, WhatsApp and Twitter. It's another case of "if it's too good to be true..." The best action is to delete the message or email. Alternatively, check the official website of the supermarket or their official social media accounts. If they are offering a deal, the likelihood is you'll find the details there.

---

## 11. Romance Scams

Looking for festive love online? Criminals are. Or you may have been approached through social media such as Facebook or Instagram by someone you don't know. The relationship develops over time and the individual is convinced to make payments to the criminal - DON'T pay them anything. They're also after your identity. Guard your privacy.

---

## 12. NHS Covid-19 Scams

Look out for potential NHS Covid-19 scams, in the past criminals have used text messages, phone calls, fake websites and even home visits to try and trick people into making a payment or handing over their financial information. This could be for things like the Covid pass, Covid jabs including the booster jab, and even the NHS app.
Fraudsters will try and convince you that you must "pay" for these things, but they are all available from the NHS free of charge.

---

# 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 on: www.facebook.com/leicstradingstandards

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