Trading Standards Scams News

A round-up of the latest scams alerts

Leicestershire County Council

October 2021

Welcome….

to the October 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.

NHS Covid-19 Scams

As we approach winter, 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 have to "pay" for these things, but they are all available from the NHS free of charge.

Remember the NHS will never:

⚠ **Ask for payment or bank details**

⚠ **Arrive unannounced at your home**

⚠ **Ask for copies of personal documents to prove your identity**

More information can be found on the NHS website links below;

https://www.nhs.uk/conditions/coronavirus-covid-19/covid-pass/

https://www.nhs.uk/conditions/coronavirus-covid-19/coronavirus-vaccination/coronavirus-booster-vaccine/

No Cold Calling Door Stickers

We would like to remind residents that Leicestershire TS can provide no cold calling door stickers as a deterrent for those who may be experiencing doorstep callers.

The door stickers could be useful for those who may live alone or be particularly vulnerable to cold callers.

If you, a family member, friend or neighbour could benefit from having one of these door stickers, you can request one by calling 0116 305 8000 or email tradingstandards@leics.gov.uk

---

Shopping Online Safely

With shorter days and longer nights drawing in, and Christmas fast approaching, this gives us more time to spend online looking for bargains.

Being scam savvy will help you know what to look out for. Here are some of the risks of online shopping to be aware of:

- ! Fraud resulting from making payments over unsecured web pages or using an unsecure Wi-Fi connection
- ! Bogus online stores or shops – fake websites and email offers for goods and services that do not exist.
- ! Buying fake goods – even if unintentional, or they are of substandard quality. This could also possibly be funding more serious crimes in the process.
- ! Losing money when you make direct bank transfer payments, only to find that the goods are inferior, or do not exist at all.
- ! Receiving goods or services which do not match the advertiser's description.
- ! Being offered tailored prices based on information gathered by the retailer about your online shopping habits and websites visited.

So, what are that steps that you can take to keep yourself safe from online shopping scams?

- ✓ **Choose carefully where you shop -** Research retailers online to make sure they're legitimate and beware of fake shopping websites.
- ✓ **Make sure the website is secure –** A padlock next to a website's URL 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://
- ✓ **Keep your devices and software up to date –** by installing the latest software and app updates. These usually contain important security updates that can protect you against

fraud and identity theft. You may be able to turn on automatic updates so your device will update itself in future.

- ✓ **Keep your email and online accounts secure** – By using different passwords for different accounts and using strong passwords, this will help to ensure that if one of your accounts is hacked, the fraudsters won't be able to access your other accounts. You can further protect your important accounts from being hacked by turning on two-factor authentication (2FA). Turning on 2FA stops hackers from accessing your accounts, even if they know your password. It does this by asking you to confirm that it's really you in a second way - usually by asking you to enter a code that's sent to your phone.

- ✓ **Use a credit card to make online purchases –** This may provide you with some level of protection if things go wrong. You could also consider using an online payment platform, such as PayPal, Apple Pay or Google Pay. Using these platforms to authorise your payments means the retailer doesn't see your payment details.

- ✓ **If things go wrong -** The first step, if you have been sent the wrong or defective items, should be to contact the online seller or the website.
  If you paid on card and you're not happy with the retailer's response, or you have received no response, contact your card provider.
  If you think your card has been used fraudulently, let your bank know straight away so they can stop it being used any further.
  As long as you haven't acted fraudulently or negligently, you'll usually get your money back from your card company if your card details are used online by a criminal to commit fraud.

Spam & Scam Emails & Texts….

You may have subscribed to receiving communications from organisations and companies that you deal with. Amongst these genuine messages, there may well be fake ones, containing links designed to steal your money and personal details that can be very difficult to spot. Fraudsters do this by pretending to be someone you trust, or from an organisation you trust. Examples of this could be your telephone or internet service provider, a utility company, banks, HMRC, parcel delivery companies. And they may contact you by phone call, email or text message. The term 'phishing' is often used when talking about emails.
Not all messages are bad, but if something doesn't feel right, follow these tips:

- If you have received an **email** which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) at **report@phishing.gov.uk**.
- If you've received a suspicious **text message**, forward it to **7726**. It won't cost you anything and allows your provider to investigate the text and take action (if found to be a scam).
- If you come across an **advert** online that you think might be a scam, report it via the Advertising Standards Authority (ASA) website. This allows ASA to provide online service providers with the details they need to remove these from websites.

Blue Badge Scams

Following a recent report to Leicestershire Trading Standards, we would like to warn residents about blue badge application scams. Whilst a blue badge application is free (£10 if a badge is issued), some people can find the process a little daunting. This is when the scammers step in by offering to apply for a blue badge on your behalf. They use a variety of methods to con people into feeling that the application fee is money well spent, by using methods such as official-looking websites, convincing website addresses, and exaggerated claims about how hard the process is. The amount the scammers charge for submitting an application for a Blue Badge on your behalf varies, but it's normally around £50, and some don't even forward your application on your behalf once you've paid. This could mean you have handed over your money for nothing and will still need to apply through the official channels yourself.

Spotting a Blue Badge scammer is easy, if the website address doesn't end in GOV.UK or a local county council website (which will end in 'gov.uk' too), then it's a scam.

It doesn't matter how official the website appears to be if it doesn't end in gov.uk it's not an official website and is almost certainly a scam. For further information from the official government website, please see below:

https://www.gov.uk/apply-blue-badge

Finally…..

If you would like to report 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