

19 May 2025

Lloyds highlights 'too good to be true' offers on social media, to help people spot scams

Ahead of the end of May Bank Holiday and summer season, Lloyds is highlighting the latest social media scam, to help people spot these 'too good to be true' offers.

How the scam works

As the Bank Holiday approaches, social media scammers have been posing as DIY companies and other well-known retailers, offering too-good-to-be-true deals in the knowledge many DIY-ers are getting ready to put the Bank Holiday and summer season to good use.

The fraudsters are placing adverts on Instagram and Facebook, pretending to be from recognisable names including Screwfix, Amazon, Decathlon and Elemis.

These fake adverts claim there is a time-limited offer for products at very low prices, with people asked to click through to enter a 'draw' or pay a small amount (e.g. for postage). The fraudsters also post fake reviews underneath the adverts, pretending to be people who have received the cheap products or deals.

The product never arrives, but the fraudsters use the information gathered to sign people up to monthly card payments – known as a 'continuous payment authority', for non-existent services.

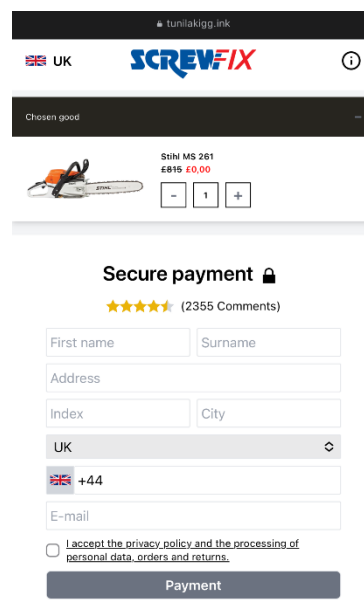
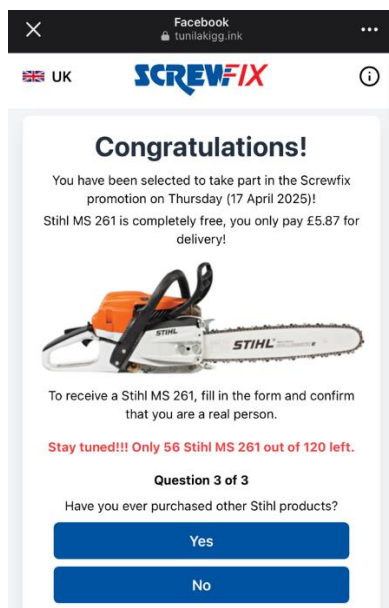
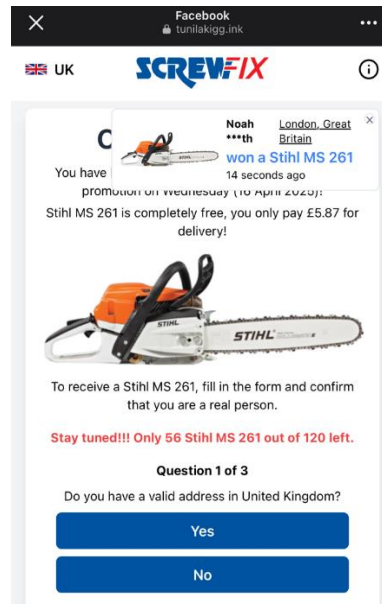
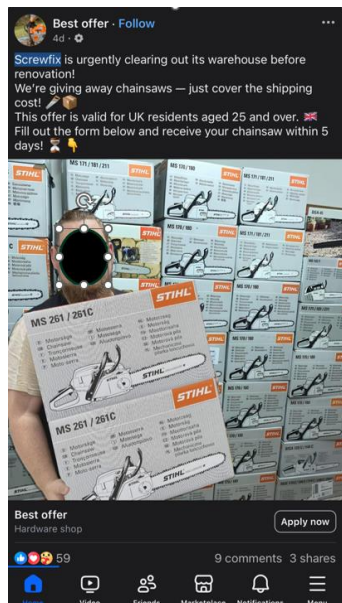
People often only become aware of the scam later, when they notice unusual card transactions – typically between £30 to £40 every two to four weeks - on their statement.

While the statement entries differ, around 80% of the payments appear with the code *PYD* and, where location services are available, usually show as based in Cyprus ('CYP' on the statement) or Ireland ('IRL').

Here's the scam in action, using stolen logos from legitimate retailer, Screwfix

Contact

Olwen Jones-Lowe | olwen.jones-lowelloydsbanking.com |



Other fake adverts to look out for

Lloyds is highlighting other ‘too good to be true’ adverts on Instagram and Facebook, so people can protect themselves:

- Decathlon – fraudsters claim the retailer is selling off old stock to make room for new collections,

Contact



with old bikes going for £1.87. People are told to hurry and click a link, so they don't miss out on the promotion.

- Amazon – this is the same MO as Decathlon, with fraudsters claiming Hp laptops are available for £1.87 to make way for new stock, with people asked to follow a link to take advantage of the 'exclusive' offer.
- Elemis Beauty – this one is slightly different, with fraudsters saying the retailer is testing new products and is offering free kits, with participants having to pay a small charge for delivery only.

In all cases, following the link directs people to a payment form, where card details are requested. The scammers use this information to sign people up to non-existent services and products, which charge the card every month.

How many reports have been received?

Between the 1st of January 2025 and 24th April 2025, Lloyds has seen around 1,400 chargeback requests from credit card customers, who spotted unusual card transactions on their statement, after signing up for a deal on social media platforms. This has led to £55,000 being charged back to the scam merchants.

Lloyds analysed the merchants appearing in the chargeback requests from customers and found around 30% of customers who had made credit card payments to these merchants between 1st Jan and 24th April, had raised a chargeback.

Lloyds predicts a further c.£144,000 could be charged back to these merchants and are encouraging people who have recently signed up to one of these deals to check their card statement and to get in touch if they see anything they don't recognise, with customers able to easily raise queries about transactions in the mobile app.

Gavin Evans, Senior Fraud Manager at Lloyds, said: "These scammers are pretending to be trusted, legitimate retailers to make people think they're getting a great deal, but there are some clear warning signs people can look out for, when these ads pop up on social media. The biggest one is the offer is always too good to be true, with expensive goods apparently available at incredibly low prices, with no sign of the deal on the merchant's website.

"If you do notice an unusual card transaction on your statement, always get in touch with your bank - Lloyds customers can get quick and easy support with unrecognised transactions by tapping on the payment in their mobile app, then pressing the 'get help with this transaction' button.

"In many cases, card protections will apply – which means your bank can reverse the charge back to the scammer."

Contact



Gavin's tips for staying safe:

- **Too good to be true:** Be wary of any advert on social media that claims to offer extremely low prices for goods that are typically much more expensive or deals that claim the payment is for 'postage only.' Go to the retailer's official website to see if they have any offers on and, if you can't find any evidence of the ones you see on social media, it's a scam.
- **Time limited:** Scam adverts almost always have a time limited angle, claiming that products are running out, or the offer is for only a few days. Legitimate retailers will not pressure you into making purchases, so take the time to check all details carefully.
- **Strange links:** Fraudsters want to get you away from social media and onto their websites, to harvest your card or other personal details. Keep an eye on the web address at the top of the page – if the address looks odd, includes a company name that you don't recognise, or is similar to a legitimate retailer but not quite right, it's more than likely a scam.
- **Examine the small print:** Some of the payment processing screens include small print which explains you are consenting to ongoing payments. Where there is small print, pay close attention to what it says, as it can help with understanding exactly what you're being asked to pay for.

Ends

Notes to Editors

Data analysed is from Lloyds Banking Group credit card customers, between 1st Jan 2025 and 24th April 2025.

'Get help with this transaction' button also available in the Halifax and BoS mobile apps.

Contact

Olwen Jones-Lowe | olwen.jones-lowel@lloydsbanking.com |