ONLINE BARGAIN HUNTERS URGED TO STAY SAFE FROM SOCIAL MEDIA SCAMMERS

- A third of people have been duped by scammers on social media
- Victims have lost an average of £393
- 45% have transferred cash but never received the goods

Online bargain hunters are being urged to watch out for festive fraudsters as more than a third (34%) of Brits have been scammed buying from social media sites.

New research from Lloyds Bank revealed that the average amount people are being tricked into handing over on social media is £393, whilst 45-54-year-olds are being scammed out of £498 on average.

The poll of more than 2,000 UK adults found almost half of people had sent money via bank transfer to sellers on social media platforms yet never received their items.

More than one in five (21%) have bought an item on an online marketplace via bank transfer and never received it. One in eight have bought something in a social media group that didn’t arrive, whilst 12% have clicked on a link shared on social media and bought goods that were never delivered.

The research revealed a lack of understanding around the safest ways to pay for goods online, as social media scammers can often trick buyers into paying by bank transfer. More than half of people (55%) think that a bank transfer is a safe payment method, when in fact paying via credit card offers much greater protection.

The top three most popular items bought by shoppers via social media are clothing (37%), toys (19%) and tickets (17%).

Those looking to make last minute Christmas present purchases are being urged to stay safe by using cards and secure payment methods, as well as taking steps to protect themselves from would-be scammers.

Paul Davis, Retail Fraud Director, Lloyds Bank, said: “Scammers are ready to take advantage of anyone letting their guard down online in the Christmas shopping rush, so it’s more important than ever to stop and think about how you’re paying when buying through social media.

“The safest way to pay for things online is by card. Paying by bank transfer is just like handing over cash, so it’s crucial to think before handing over your money – and remember that any offer which seems too good to be true probably is.
“Always ring the number on the back of your bank card if you’re not sure and remember your bank will never ask for your personal details or for you to transfer money to another account. If you’re worried you’ve been a victim of a scam, contact your bank immediately so they can try to recover your money.”

Consumer shopping habits around the festive period could leave people more vulnerable to social media scammers, as more than one in five (23%) say they have shopped on websites that they have never used before in the lead up to Christmas. Meanwhile, 16% have bought items from sites they wouldn’t normally use, and 15% have bought Christmas presents via social media platforms that they wouldn't normally use.

Although people enjoy the convenience of shopping online via mobile and tablet device, those who don’t stop to check where their money’s going could be left out of pocket. More than one in four said that if they see something they want and it’s cheap, they will buy it immediately, whilst 61% are not bothered about buying from well-known sites.

Mike Haley, CEO of fraud prevention organisation Cifas, said: “The ease and speed by which we can now buy goods on our phones and other devices means we often make ourselves more vulnerable to fraud without even realising it.

“Fraudsters are always ready to take advantage of anyone who lets their guard down and be wary of deals that seem too good to be true. Never feel pressured into sharing information – whether personal or financial – however good a bargain might appear.

“Stay alert to beat the fraudsters this Christmas to make sure they’re the only ones left short-changed over the festive period.”

TIPS TO HELP SHOP SAFELY THIS CHRISTMAS

1. Keep your physical card safe and on you at all times – do not hand it over when making a payment
2. Shop smart – use trusted online retailers, and make payments by credit card where possible
3. Use a safe connection – ensure your devices are protected and avoid using unsecured WiFi networks
4. Give your bank your mobile number – many banks will ask you to verify payments by SMS
5. Explore if your bank offers card controls – Lloyds Bank, Halifax and Bank of Scotland app users can freeze their card instantly to stop it being used
6. Be cautious about any unexpected calls or messages you receive – don’t click on links or give out personal details. If you’re ever in doubt, call your bank using the number on the back of your card
7. Check your bank statements regularly – if you spot anything suspicious, report it to your bank immediately
How Lloyds Bank tackles fraud

Lloyds Bank (part of Lloyds Banking Group) has a 24/7 team dedicated to protecting customers from fraud.

Our branch and telephone banking colleagues are specially trained to identify signs that could indicate that a customer could be a victim of fraud.

We launched a mule-hunting team to detect and stop money mules at the start of 2018. The team’s mission is to stop the movement of money from scams, shutting down fraudsters’ attempts to shift money using cutting-edge defences developed by specialists from across the bank. The team has frozen £18.5m so far and returned £4m to victims.

As part of this industry-leading pilot, the team developed a number of new techniques to rapidly analyse data, spotting tell-tale signs, patterns and behaviour to halt fraudsters in their tracks. For all of the frozen funds, we are contacting the sending banks in order to help them get the money back to victims.

We are a leading supporter of Take Five (led by UK Finance) – a campaign urging people to stop and think before giving out their personal details and making transactions.

We support the industry-wide voluntary code on APP scams to help protect victims of fraud. Our priority is keeping customers’ money safe from scams by stopping fraud from happening in the first place. We will ensure that our customers who have done the right thing and followed the best practice in the new code will always be refunded.

ENDS

Note to editors:
The research was carried out online by Research Without Barriers between 8th November 2019 and 12th November 2019. The sample comprised 2,007 UK adults. All research conducted adheres to the UK Market Research Society (MRS) code of conduct (2019). RWB is registered with the Information Commissioner’s Office and complies with the DPA (1998).