Editor: RACHEL RICKARD STRAUS
www.thisismoney.co.uk

The five sneakiest BLACK FRIDAY SCAMS and how to avoid them

By **Helen Kirrane**

BLACK Friday this week is tipped to be the busiest on record as millions of shoppers look to grab online bargains.

As many as three in five people will be shopping for deals in the Black Friday sales. But beware — today the boss of Barclays bank warns that an 'unprecedented' rush of scammers will try to prey on those looking for a bargain this year, particularly online.

Risk analysts at data firm LexisNexis Risk Solutions say customers should prepare for an 'onslaught of fraudulent attacks' as the Black Friday bonanza gets under way.

Here Money Mail reveals the top five Black Friday scams you need to watch out for — and how you can protect yourself...

1. Incorrect bank details swindle

THIS growing scam involves fraudsters emailing shoppers to say that there has been a problem with their transaction that needs correcting immediately.

The email will purport to be from a retailer that you may have recently bought from, telling you that some of the billing information you provided is incorrect. The scammer hopes that you will click on a link in the email to enter your bank details and other personal information. Once they have this, they may use it to carry out fraudulent transactions in your name.

Or they may contact you later claiming to be from the police, your bank or another trusted authority and use the information that you have handed over to convince you that they are genuine.

This type of scam will be particularly successful during Black Friday due to the sheer quantity of shoppers making purchases. That is because scammers tend to send the same bogus email to tens of thousands of potential victims claiming to be from a large retailer.

If you have not bought from that retailer recently, there is a good chance you will ignore the email.

But if you have, it could strike a chord and you're more likely to fall prey.

If a retailer asks you to change your bank details with urgency and claims there is a risk of losing out on an order you have made, then you should be suspicious.

2. Fake goods and purchase con

A PURCHASE scam is where you make a payment for goods or services that are fake or never turn up. Shoppers are particularly at risk of falling victim to purchase scams during Black Friday as they are in the mindset of hunting down bargains and getting good deals on Christmas presents for loved ones.

Money Mail
STOP THE SOCIAL MEDIA SCAMMERS

More than one in four parents have been tricked by purchase scams in the past according to trade body UK Finance. They are particularly likely to be susceptible, as fraudsters often take advantage of the fact that lots of parents will be trying to track down a popular present for their children.

Fake goods are most commonly advertised on Instagram or Facebook Marketplace. Money Mail is campaigning for social media companies to better protect users, and has revealed just how easy it is for scammers to target victims on their platforms.

According to Lloyds Bank, the most common items listed in fake ads or posts for Black Friday include Apple iPhones, Nintendo Switches, Nike trainers, PlayStations, Lego sets and drones.

Be wary of offers that seem too good to be true.

Check customer reviews of the seller to make sure they have a good track record.

3. Tracking number trick

IN THIS type of scam, a fraudster will send fake text messages or emails containing links, pretending to be from a retailer or courier with fake parcel tracking information.

Scammers take advantage of the fact that shoppers are likely to have lots of parcels arriving at this time of year.

If you click the link or open the attachment, crooks can then infect your device with malware or direct you to fake websites where they will trick you into handing over your personal details.

Jodie Wilkinson, from card payment firm TakePayments, says: 'An influx of Black Friday online orders can cause delays with delivery. Scammers may take advantage of this by sending out delivery update emails with messaging like "There's a problem with your delivery", or "Click here for a delivery update", with a link in a fraudulent email.'

Stop and think before you click on any links contained in an email.

4. Brute force computer attacks

RETAILERS will see surges in 'brute force attacks' this year, according to LexisNexis Risk Solutions. This is where fraudsters attempt to break into customer accounts by using technology that can attempt to guess their password and log in details millions of times a second.

If a company with which you have an account contacts you to say your password has been changed, tell the firm immediately if it wasn't you.

If you have a debit or credit card linked to that account, you may want to ask your bank to put a temporary freeze on it to prevent any unauthorised payments.

5. Bogus discount codes and offers

DURING Black Friday, consumers are bombarded with messages from retailers promising deals.

Scammers often replicate these messages from big-brand names. They send emails or text messages including fake discount codes or links to counterfeit websites.

If you want to take advantage of a Black Friday deal and are not sure if an offer you have seen is genuine, go directly to the retailer's website.

We're braced for gangs of crooks targeting shoppers

FINDING that Black Friday deal online will be this week's highlight for thousands of Barclays customers.

Unfortunately, the sheer volume of shoppers looking for a bargain will attract an unprecedented number of criminals ready to scam them. We at Barclays, like other UK banks, are braced. We warn customers to be vigilant, but our data shows that money lost to purchase scams surged by 22pc during the Black Friday and Cyber Monday weekend last year. Victims were robbed of £970 on average.

And it doesn't stop there. Hundreds of millions of pounds are lost to scams every year because of the co-ordinated attacks of organised crime gangs. But efforts to prevent this crime lack the same co-ordination, with the Government, regulators, the banks and tech firms working in siloes. This fragmented fight against scams allows criminals to slip through the cracks and take advantage of the lack of data sharing between these different groups.

By **Matt Hammerstein**
CEO OF BARCLAYS UK

We wholly support the Daily Mail's 'Stop the Social Media Scammers' campaign and urge the Prime Minister to bring together a united, cross-Government group empowered by our new Home Secretary and the Chancellor, and rally regulators, policymakers, industry groups, and companies across different sectors to effectively fight scams. Banks cannot win this fight alone. We need the Government to look at how and where scams occur.

Barclays data shows that nine in ten scams happen on tech platforms. Yet it is only banks that publicly publish data relating to scams. We must work together to stamp out this criminal activity, which is hurting countless individuals and jeopardising our economy and its future growth. Organised criminal scam gangs might be strong but, by working together, with the Government leading the charge, we can be even stronger.

HOW TO STOP SURGE PRICING BLOWING YOUR BUDGET SEE NEXT PAGE