# Scotland Yard investigates M&S cyber attack by teenage hacker group



Scotland Yard detectives are investigating a significant cyber attack that has crippled Marks & Spencer (M&S), with the IT disruption believed to have been orchestrated by a teenage hacker group known as Scattered Spider. The Metropolitan Police’s cyber crime unit has been engaged in the probe, working alongside the National Cyber Security Centre and the Information Commissioner’s Office (ICO) to understand and counter the attack.

This cyber group, reportedly comprising around 1,000 mainly British and American youths and young men, has garnered a notorious reputation globally for targeting major brands with sophisticated attacks. Cyber security experts have highlighted the group’s dangerous level of expertise, combining technical hacking skills with social engineering tactics, such as phishing scams designed to manipulate company staff and IT help desks into providing access to corporate systems.

According to reports from the trade website Bleeping Computer, Scattered Spider is believed to have infiltrated M&S’s servers as early as February and then executed the attack around the Easter period. The fallout has forced M&S to pause its click and collect service, significantly disrupting its online ordering capability. The retailer’s home and clothing segment, which typically generates approximately £11 million in daily sales, with a third coming from online sales, faces substantial financial losses estimated at nearly £3.7 million per day while the online platform remains offline.

M&S has reportedly sought assistance from cyber security experts, including Microsoft, CrowdStrike, and Fenix24, in its efforts to restore services and secure its systems. Despite the disruption, the company has refrained from commenting on the specifics of the attack, including the identity of the hackers or whether any ransom demands have been met. Industry insiders note that such criminal groups often demand ransoms of up to £10 million in exchange for restoring full access to affected companies' IT systems.

The hacker collective, also known by names such as Scatter Swine and Muddled Libra, has a history of targeting numerous firms since May 2022. Last year, US authorities charged five alleged members related to attacks on at least a dozen companies, including the high-profile case of casino operator Caesars Entertainment, which was forced to pay hackers £12 million in 2023 following a similar cyber attack.

Among the suspects is Tyler Buchanan, a 22-year-old from Dundee who was extradited from Spain to California on charges linked to casino cyber attacks. Previously, a 17-year-old from Walsall was arrested in connection with global investigations into Scattered Spider activities. Recently, a leading member of the group, Noah Urban, pleaded guilty to multiple online fraud offences in a Florida court, facing up to 60 years in prison and an order to repay more than £10 million.

Business leaders have expressed concern about the broad-reaching threat posed by cyber criminals. George Weston, chairman of Associated British Foods, which owns Primark and Twinings tea, commented on the situation in an interview with the Daily Mail, saying, “All of business, certainly us, have been very aware of cyber risk for some time... We look at what’s happened [at M&S] with sadness. Whatever we can do to help, we would do – but it’s a threat to all of us.”

Meanwhile, the operational impact on M&S remains significant, with stores experiencing empty shelves and the online service suspended for the fifth day. The ongoing investigation and recovery efforts continue, with no arrests made at this stage, as authorities seek to bring those responsible to justice and restore normal service to one of the UK’s leading retailers.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.reuters.com/business/retail-consumer/britains-ms-says-cyber-attack-has-hit-food-availability-some-stores-2025-04-29/> - This article reports that Marks & Spencer (M&S) disclosed a cyber attack that disrupted food item availability in some of its stores, leading to the suspension of online clothing and home orders via its website and app.
2. <https://www.ft.com/content/1d46953a-5f2d-4395-85b9-af337a4747db> - The Financial Times article details how the cyber attack on M&S resulted in nearly £700 million being wiped from its market valuation, with the company halting online clothing and homeware orders and experiencing issues with contactless payments and store returns.
3. <https://www.reuters.com/technology/cybersecurity/ms-tells-warehouse-agency-staff-stay-home-cyber-incident-continues-2025-04-28/> - This Reuters report states that M&S instructed approximately 200 agency staff at its Castle Donington distribution center to stay home due to the ongoing cyber incident disrupting its online operations.
4. <https://www.reuters.com/business/retail-consumer/british-retailer-ms-discloses-cyber-incident-2025-04-22/> - The article reports that M&S disclosed a cyber incident it had been managing over the past few days, implementing temporary changes to its store operations in response to the issue.
5. <https://www.computing.co.uk/news/2024/security/scattered-spider-suspects-indicted> - This article discusses the indictment of five individuals believed to be part of the Scattered Spider cybercrime gang, who are accused of orchestrating a multi-million-dollar phishing and hacking scheme.
6. <https://thehackernews.com/2023/10/microsoft-warns-as-scattered-spider.html> - The Hacker News article highlights Microsoft's warning about Scattered Spider expanding from SIM swapping to ransomware attacks, detailing the group's sophisticated social engineering tactics and their impact on various sectors.
7. <https://www.dailymail.co.uk/news/article-14661627/Notorious-hackers-M-S-cyber-raid-Retail-giant-calls-Scotland-Yard-finger-pointed-gang-blackmails-firms-millions.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data