# Scotland Yard investigates cyber attack causing major disruption at M&S



Scotland Yard has launched an investigation into the cyber attack that has severely disrupted operations at Marks & Spencer (M&S), causing empty shelves in stores and a significant decline in the retailer's market value. The Metropolitan Police confirmed they were called to address the incident on Wednesday, 23 April. Detectives from the Met’s Cyber Crime Unit are actively investigating the case, which remains ongoing.

The retailer is also collaborating with experts from the National Crime Agency (NCA) and the National Cyber Security Centre (NCSC). According to the NCA, these organisations are working closely to better understand the nature of the cyber incident and offer support to M&S.

M&S first disclosed the attack on Tuesday, acknowledging “pockets of limited availability” of certain items in some stores. The disruption followed the retailer’s precautionary decision to take some systems temporarily offline to mitigate the effects of the breach. Since the cyber attack began over a week ago, M&S has faced complications with its contactless payments and click-and-collect services, which led to a temporary suspension of orders on its website and app from last Friday. These services have remained offline as the company works to resolve the issue.

A spokesperson for the Metropolitan Police said: “We were called on Wednesday, 23 April regarding a cyber-incident at Marks & Spencer. Detectives from the Met’s Cyber Crime Unit are investigating. Enquiries continue.”

Professor Alan Woodward, a cyber security expert at the University of Surrey and former adviser to Europol, spoke to The Independent on Tuesday, providing insights into the prolonged nature of the disruption. Prof Woodward explained that M&S’s cautious approach in investigating the incident likely explains the extended downtime: “They are turning over every rock and making sure there’s nobody still in there. Because one of the worst things is if a hacker has got in, let the ransomware go, and they can persist on the network, then you might clear it – you might get out of it – but they’ll just pop back up again.”

Reports have linked the cyber attack to a hacking group known as Scattered Spider, reputedly involving British and American teenagers. Tech news outlet Bleeping Computer was among the first to associate this group with a potential ransomware attack against the retailer. Furthermore, investigators reportedly believe that the attackers utilised a hacking tool from DragonForce, a group describing itself as a “ransomware cartel,” to execute the breach, according to The Telegraph.

M&S has not confirmed specific technical details of the attack but continues to work intensively with law enforcement and cybersecurity experts to restore normal operations. The incident remains a significant challenge for one of the UK’s leading retail brands, impacting customer services and the company’s financial standing in the market.

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

## Bibliography

1. <https://www.reuters.com/business/retail-consumer/britains-ms-pauses-some-online-orders-after-cyber-incident-2025-04-25/> - This article reports that Marks & Spencer (M&S) temporarily halted online orders in the UK and Ireland following a cyber attack, leading to a 5% drop in its share price. The company emphasized that its physical stores remained open and that it was working with cybersecurity experts to restore digital services.
2. <https://www.reuters.com/business/retail-consumer/britains-ms-says-cyber-attack-has-hit-food-availability-some-stores-2025-04-29/> - This report details how M&S disclosed that a cyber attack disrupted food item availability in some of its stores. The incident prompted M&S to halt clothing and home orders via its website and app, following issues with contactless payments and click-and-collect services over the Easter weekend.
3. <https://www.reuters.com/technology/cybersecurity/us-charges-five-scattered-spider-hacking-scheme-2024-11-20/> - This article discusses the U.S. charges against five individuals connected to the hacking group known as Scattered Spider, alleging their involvement in a series of phishing attacks targeting employees of various U.S. companies to steal login credentials, confidential information, and cryptocurrency.
4. <https://www.reuters.com/world/uk/britains-co-op-is-latest-retailer-to-be-hit-by-cyber-attack-2025-04-30/> - This piece reports that the Co-op Group in Britain became the latest retailer targeted by a cyber attack, prompting the company to shut down some back office and call centre operations as a precaution. Despite the attack, all Co-op stores, e-commerce services, and funeral homes continued to operate normally.
5. <https://www.sky.com/story/scottish-man-linked-to-hacking-group-scattered-spider-among-five-charged-in-us-13257514?dcmp=snt-sf-twitter> - This article reports on the arrest of a 22-year-old British national, allegedly the leader of an organized group dedicated to stealing information from companies and cryptocurrencies, who was arrested at Palma airport in Majorca.
6. <https://www.informationweek.com/cyber-resilience/suspected-scattered-spider-leader-snagged-in-law-enforcements-web> - This piece discusses the arrest of the alleged leader of the Scattered Spider hacking group, highlighting the group's focus on identity and access management systems and their use of social engineering tactics, including SIM swapping attacks.
7. <https://www.independent.co.uk/news/uk/crime/m-s-cyber-attack-met-police-b2742155.html> - Please view link - unable to able to access data