# Hackers disrupt Marks & Spencer online services in £30 million cyberattack linked to geopolitical motives



Hackers have unleashed a significant cyber assault on Marks & Spencer (M&S), causing severe disruptions to the retail giant’s online services and raising questions about the motivations behind such attacks. The cybercrime group DragonForce has claimed responsibility for this sophisticated breach, amidst revelations regarding its political leanings and a concerning rise in digital crime targeting UK retailers.

The hacking incident, which has hampered M&S's ability to process online orders for clothing and home products, began when criminals impersonated employees to trick IT help desks into resetting passwords, thereby gaining unauthorised access to internal networks. Following the breach, Marks & Spencer was forced to suspend its click and collect service, leading to a 12% decline in its share price. Financial analysts estimate the impact of the attack could reach approximately £30 million, with ongoing losses potentially amounting to £15 million per week. The delays have not only affected online shopping but also resulted in limited stock availability in physical stores.

DragonForce, which describes itself as aiming to "just take some money and walk away," hinted at broader political intentions in a recent statement. It warned against the use of its ransomware against critical infrastructure in the former Soviet Union, suggesting that it would impose consequences on anyone violating this stance. Its declaration added an unexpected layer of complexity to the situation, indicating a potential geopolitical dimension to what is typically viewed as economic-driven cybercrime.

The fallout from these cyber-attacks has not only befallen M&S but also the Co-op, which reported that personal data was extracted from its membership scheme. This breach has raised alarms within the National Cyber Security Centre (NCSC), which has since urged retailers to fortify their cybersecurity protocols against similar deception tactics. The NCSC has emphasised the importance of revising help desk procedures to prevent these types of attacks, signalling an urgent call to action for businesses operating in an increasingly vulnerable digital landscape.

Ongoing investigations suggest that the hacking group Scattered Spider may be involved as well. Notably, this younger, English-speaking group has gained notoriety for targeting large corporate entities and employing social engineering tactics to infiltrate their systems. Their exploits have not only targeted M&S but also left a trail of chaos at companies such as MGM Resorts International and Caesars Entertainment. The growing trend of teenagers participating in high-stakes cybercrime is particularly worrying, as they leverage advanced techniques including SIM swapping and phishing to achieve their criminal goals.

Cybersecurity experts warn that UK retailers are especially attractive targets for cybercriminals, given their access to vast amounts of customer data and real-time operations. The recent spate of attacks on well-known brands points to a potentially coordinated effort among different hacking groups, with many analysts speculating that they may share resources and techniques, complicating detection and prevention efforts.

While M&S has experienced substantial disruptions, it is fortunate that, thus far, sensitive financial information remains secure. Nonetheless, this incident serves as a stark reminder of the fragility of cybersecurity in today's digital age. As M&S navigates recovery, it faces not only the challenge of restoring services but also re-establishing consumer trust, which has likely been shaken by this high-profile breach.

The rise of groups like DragonForce and Scattered Spider highlights an unsettling trend in cybercrime, where economic objectives are increasingly entwined with geopolitical motivations. This duality complicates how businesses must approach their own cybersecurity strategies. Ensuring robust protection against such evolving threats will be crucial as the retail sector seeks to protect itself against the next wave of hackers.

### Reference Map

1. Paragraphs 1, 2, 3, 4, 5, 6, 7
2. Paragraphs 2, 6
3. Paragraphs 2, 4
4. Paragraphs 2, 3, 6
5. Paragraphs 4, 6
6. Paragraphs 4, 5, 6

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

## Bibliography

1. <https://www.dailymail.co.uk/news/article-14699457/hackers-target-Marks-Spencers-political-allegiance.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/> - Cyberattacks on UK retailers Marks & Spencer (M&S) and the Co-op Group were initiated by hackers impersonating employees and deceiving IT help desks into resetting passwords, granting them access to internal networks. The UK's National Cyber Security Centre has advised organizations to revise their help desk protocols to prevent similar breaches. M&S, having disclosed the cyber incident on April 22, witnessed a 12% share decline and subsequently suspended online clothing and home orders; food product availability has also been disrupted. Analysts estimate the financial impact at approximately £30 million ($40 million), with ongoing losses of around £15 million weekly. The attack has been linked to the hacking group 'Scattered Spider' using DragonForce ransomware, though the National Cyber Security Centre has not confirmed any direct connection between these incidents. ([reuters.com](https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/?utm_source=openai))
3. <https://www.ft.com/content/602e10e7-00b3-4c9b-bb27-6480d7246f37> - The UK's National Cyber Security Centre (NCSC) has issued a warning to retailers about an increase in cyberattacks involving criminals impersonating IT help desks. This alert follows recent attacks on major retailers including Marks and Spencer (M&S), Co-op, and Harrods. The NCSC emphasized the risk of social engineering tactics, in which attackers deceive IT personnel into resetting passwords, thereby gaining unauthorized access to systems. Co-op revealed that hackers extracted customer names and contact details, after initially claiming the attack was unsuccessful. As a result, Co-op is facing store shortages due to operational disruptions. M&S, similarly affected, has been unable to process online orders for over a week and is also experiencing limited stock availability. ([ft.com](https://www.ft.com/content/602e10e7-00b3-4c9b-bb27-6480d7246f37?utm_source=openai))
4. <https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9> - Several major UK retailers, including Marks and Spencer (M&S), the Co-op, and Harrods, have recently been targeted by cyber attacks, highlighting the increasing vulnerability of the retail sector. M&S has faced significant operational disruptions and a £600 million drop in value due to these attacks. Investigations are ongoing, and experts suspect a common supplier or technology could link the incidents. Cybersecurity professionals suggest a potentially coordinated effort, possibly involving the group Scattered Spider, known for manipulating individuals to gain system access. The National Cyber Security Centre has expressed concern, urging businesses to treat cybersecurity seriously. Retailers are attractive targets due to their vast customer data, real-time operations, and reliance on legacy systems. Although some customer data was accessed, sensitive financial information reportedly remains secure. Cybersecurity apathy, especially among large UK retailers, has been noted in recent industry research. Experts warn that even without paying ransoms, attackers could profit by selling stolen data. The incidents serve as a stark reminder of the growing sophistication and impact of cybercrime on the retail landscape, with recovery potentially taking months. ([ft.com](https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9?utm_source=openai))
5. <https://cyberveille.decio.ch/> - The individuals operating under the DragonForce banner and attacking UK high street retailers are using social engineering for entry. The attacks on Marks and Spencer, Co-op, and Harrods are linked. Defenders should urgently make sure they have read the CISA briefs on Scattered Spider and LAPSUS$ as it’s a repeat of the 2022–2023 activity which saw breaches at Nvidia, Samsung, Rockstar, and Microsoft amongst many others. Harrods is the latest retailer to be hit by a cyber-attack, just days after Marks & Spencer and the Co-op were targeted. The luxury department store is understood to have been forced to shut down some systems, but said its website and all its stores, including the Knightsbridge flagship, H beauty, and airport outlets, continued to operate. ([cyberveille.decio.ch](https://cyberveille.decio.ch/?utm_source=openai))
6. <https://www.cybersecurityintelligence.com/blog/scattered-spider-hacking-group-is-behind-the-attack-on-mands-8392.html> - The chaotic problems at British retail giant Marks & Spencer (M&S) are being caused by a ransomware attack believed to be conducted by threat actors known as Scattered Spider. M&S is a British multinational retailer that employs 64,000 employees and sells various products, including clothing, food, and home goods in over 1,400 stores worldwide. The retailer is dealing with some major issues, with empty shelves not replenished and delays to its online shopping services. Scattered Spider is known for its ability to target large multisite companies and breaching their data. Since the attack commenced last weekend, M&S has lost more than £700 million, wiped off its stock market valuation. Shoppers are still able to browse online and shop in M&S’s physical stores using cash or cards, but some major problems continue in stores, with gift cards not currently being accepted. Returning goods is only possible in clothing and homeware stores or via post. Food stores are not currently able to accept returns. Scattered Spider, also known as 0ktapus, Starfraud, Scatter Swine, and Muddled Libra, is a classification of threat actors that are adept at using social engineering attacks, phishing, multi-factor authentication (MFA) bombing (targeted MFA fatigue), and SIM swapping to gain initial network access on large organizations. Scattered Spider members have typically engaged in data theft for extortion and have been known to use BlackCat ransomware. This hacking group includes young members as young as 16 and is based in the UK and US, with a range of skills and the group began hacking in financial fraud and social media but now steals cryptocurrency and hacks company data in extortion attacks. Some Scattered Spider members are thought to be part of The Comm, a group involved in high-profile cyber incidents, and they use different individuals for each attack, making them difficult to track. One of Scattered Spider's biggest exploits was at the gaming giant MGM Resorts International in September 2023, when guests reported difficulty accessing rooms and using casino games. MGM operates over 30 hotel and gaming venues around the world and was alerted to a potential hack when Scattered Spider brought MGM systems to a halt after they gained access to the company's management systems and were able to deploy ransomware. MGM confirmed that, in that exploit, some customers' personal data was stolen, including names, dates of birth, and driving license numbers. In some cases, social security numbers and passport numbers were also involved. It is not known to what the extent of the attack on M&S might have compromised customer data and, if it has, there is a legal requirement for affected organizations to report this to the UK Information Commissioner's Office (ICO) under the 2018 UK Data Protection Act. ([cybersecurityintelligence.com](https://www.cybersecurityintelligence.com/blog/scattered-spider-hacking-group-is-behind-the-attack-on-mands-8392.html?utm_source=openai))