# Marks & Spencer defies cyberattack with 8% food sales growth and market share gain



Marks & Spencer (M&S) is successfully navigating a challenging landscape marked by a significant cyberattack, which has not deterred its appeal to middle-class grocery shoppers. In fact, food sales at the retailer surged in the wake of the incident, growing by an impressive 8% during the four weeks leading up to May 18—a figure that nearly doubles the growth rate of the broader grocery sector, which registered just over 4% during the same period. Analysts have deemed this performance "remarkably strong," suggesting that M&S is not only weathering the storm but actively extending its reach over competitors like Waitrose.

Despite the cyberattack, which surfaced on April 22, M&S's share of the UK grocery market rose by 20 basis points to 3.8%, signalling resilience even in the face of adversity. This incident, attributed to hackers leveraging vulnerabilities in third-party systems, temporarily disrupted its online and contactless payment services and caused significant logistical challenges. The company is anticipated to sustain losses of around £300 million due to increased costs associated with food supply disruptions and damaged customer trust. CEO Stuart Machin expressed confidence in the company’s recovery, stating, “We’ve been around for 140 years with lots of challenges. We survived that and we’ll survive this,” highlighting M&S's long-standing history of resilience.

As part of its strategy to bolster growth, M&S plans to expand its food business by converting 12 former Homebase outlets into larger food halls stocked with the entire M&S range. Many of these locations are strategically sited near affluent areas and in proximity to Waitrose supermarkets, intensifying the competition. The Godalming site is set to become M&S's largest food-only store, positioned directly across from a Waitrose, which could significantly shake up the local grocery market landscape.

In broader market terms, UK grocery inflation has risen to its highest level in 15 months, climbing by 4.1%. Factors contributing to this inflation include increased payroll taxes for supermarkets and wage hikes. This backdrop highlights the unusual strength of M&S's food business amid rising prices across the retail sector, which is likely affecting consumer behaviour as shoppers become more discerning about where to spend their money.

The fallout from the cyberattack remains significant, with the retailer expected to see operational disruptions continue until July. In recent weeks, M&S's stock has attempted to recover, though shares remain down by about 8.5% since the incident. Competition within the sector is intensifying, as rivals like Tesco and Sainsbury's also report rising sales figures, benefiting from M&S's online setbacks.

The cyberattack has also prompted M&S to reassess its cybersecurity measures. Incidents such as this highlight the vulnerabilities present in corporate infrastructure, particularly those exploited through human manipulation tactics like social engineering. Experts have noted that improving cybersecurity practices—notably integrating stringent identity verification measures and training for employees—will be critical to protecting company assets in the future.

While M&S is currently grappling with the financial ramifications of the cyber disruption, the commitment to resilience and a robust strategy focused on food sector expansion suggest a forward-looking stance. Despite challenges, the company is optimistic about maintaining its market position and delivering on its long-term strategic goals. As recovery efforts ramp up, M&S appears poised not only to withstand the immediate crises but potentially to emerge with a stronger brand presence in the grocery sector.

## 📌 Reference Map:

* Paragraph 1 – [[1]](https://www.dailymail.co.uk/money/markets/article-14767549/Marks-Spencer-winning-battle-middle-class-foodies.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[2]](https://www.reuters.com/business/retail-consumer/ms-food-sales-show-resilience-despite-cyberattack-says-nielseniq-2025-05-29/)
* Paragraph 2 – [[1]](https://www.dailymail.co.uk/money/markets/article-14767549/Marks-Spencer-winning-battle-middle-class-foodies.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[4]](https://www.ft.com/content/c9bd0a6a-eedf-4c98-8e2d-8deffd851761), [[6]](https://www.reuters.com/business/media-telecom/britains-ms-says-cyberattack-cost-400-million-2025-05-21/)
* Paragraph 3 – [[1]](https://www.dailymail.co.uk/money/markets/article-14767549/Marks-Spencer-winning-battle-middle-class-foodies.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[3]](https://www.reuters.com/business/retail-consumer/uk-grocery-inflation-hits-highest-level-15-months-2025-05-28/), [[5]](https://www.ft.com/content/4349b16a-8ec1-44d9-a295-3a51523805a8)
* Paragraph 4 – [[6]](https://www.reuters.com/business/media-telecom/britains-ms-says-cyberattack-cost-400-million-2025-05-21/), [[7]](https://moneyweek.com/personal-finance/marks-and-spencer-online-order-problems)
* Paragraph 5 – [[4]](https://www.ft.com/content/c9bd0a6a-eedf-4c98-8e2d-8deffd851761), [[5]](https://www.ft.com/content/4349b16a-8ec1-44d9-a295-3a51523805a8)

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

## Bibliography

1. <https://www.dailymail.co.uk/money/markets/article-14767549/Marks-Spencer-winning-battle-middle-class-foodies.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-food-sales-show-resilience-despite-cyberattack-says-nielseniq-2025-05-29/> - Despite a recent cyberattack, Marks & Spencer's food business demonstrated strong performance, with sales increasing by 10.8% year-on-year in the 12 weeks leading up to May 17, 2025, according to NielsenIQ. The retailer’s share of the UK grocery market rose by 20 basis points to 3.8%. However, the growth rate slowed compared to the 14.7% increase reported in the previous NielsenIQ period. The cyberattack forced M&S to halt online clothing orders and shut down other systems, negatively affecting food availability and increasing waste and logistics costs. As a result, the company projected a loss of about £300 million ($404 million) in operating profit, with service disruptions likely to continue until July. NielsenIQ’s data aligns with findings from Kantar, which showed strong sales growth from competitors like Aldi, Lidl, Tesco, Sainsbury’s, and Ocado. Notably, M&S is not fully represented in Kantar's market data.
3. <https://www.reuters.com/business/retail-consumer/uk-grocery-inflation-hits-highest-level-15-months-2025-05-28/> - UK grocery price inflation rose to 4.1% in the four weeks to May 18, 2025, marking its highest point in 15 months, according to market researcher Kantar. This increase, up from 3.8% in the previous month, is attributed to heightened supermarket payroll taxes and a national minimum wage hike implemented in April. The Institute of Grocery Distribution predicts food inflation might reach nearly 5% this year. Despite inflation, grocery sales climbed 4.4% year-on-year, with consumer behaviors shifting notably when inflation exceeds the 3% to 4% range. Prices surged most in chocolate confectionery, suncare, and butters and spreads, while declining most in pet food and household paper goods. Among retailers, Tesco led with 5.9% sales growth, followed by Sainsbury's at 4.7%. Asda lagged with a 3.2% sales drop but showed improved performance. Discounters Aldi and Lidl recorded their strongest combined growth since January 2024 at 8.4%. Online grocer Ocado experienced the fastest growth among all, with a 14.9% increase, and Marks & Spencer posted a 12.3% rise despite a cyberattack.
4. <https://www.ft.com/content/c9bd0a6a-eedf-4c98-8e2d-8deffd851761> - A recent cyber attack on Marks and Spencer (M&S) underscores the growing vulnerability of businesses to cyber threats. The attack, attributed to the hacker group Scattered Spider, disrupted services including online clothing sales and contactless payments, with the company facing a potential £300 million hit to operating profits. The breach, linked to third-party human error, exposed customer data and has prompted a class action lawsuit. M&S is still recovering, expecting full operational restoration by July. Cyber attacks like this—often involving ransomware that encrypts vital data—represent a form of asymmetric warfare against unprepared corporate infrastructures. Many companies grapple with outdated or patched-together IT systems and rely on external vendors. Experts stress that while total prevention is unlikely, better practices such as software updates, multi-factor authentication, backups, and operation segmentation can mitigate damage. Building cyber resilience through early detection, response, and containment is essential. More than half of UK businesses faced cyber attacks in the past five years, highlighting the need to expect disruptions and prepare systematically to endure them.
5. <https://www.ft.com/content/4349b16a-8ec1-44d9-a295-3a51523805a8> - Recent cyber attacks, including a significant one on British retailer Marks and Spencer (M&S), highlight that humans remain the weakest link in cybersecurity. M&S reportedly lost up to £300 million in profits and saw its market value drop by £750 million after criminals exploited social engineering tactics through a third-party supplier. These methods involved deceiving IT staff into resetting passwords or authentication processes. Other UK retailers like the Co-op and Harrods have also been targeted by a group known as Scattered Spider, previously linked to attacks on major US companies. Unlike traditional state-linked cybercriminals, Scattered Spider includes English-speaking hackers based in the UK and US and uses human manipulation tactics such as impersonation and SIM swapping. Despite M&S increasing cybersecurity investment and staffing, their systems were still breached, underscoring the vulnerability of supply chains and human error. Businesses are urged to prioritize cybersecurity at the board level, enforce stricter identity verification, improve staff training, impose standards on third-party vendors, and maintain a robust, rehearsed incident response plan. As commercial entities increasingly become targets, the cost of inadequate cybersecurity can far outweigh preventive investments.
6. <https://www.reuters.com/business/media-telecom/britains-ms-says-cyberattack-cost-400-million-2025-05-21/> - Marks & Spencer (M&S), a major British retailer, announced that a sophisticated cyberattack will reduce its operating profit by approximately £300 million ($403 million), with disruptions expected to persist into July. The attack temporarily shut down M&S's online clothing operations, disrupted food supplies, and wiped over £1 billion from its market value. Although online sales in the fashion, home, and beauty sectors were heavily impacted, in-store sales remained stable. The food division experienced reduced availability and higher logistics costs due to reverting to manual operations but has since shown signs of recovery. M&S aims to mitigate half of the profit loss in the 2025/26 fiscal year through insurance and cost management. Shares in the retailer fell by 13% since the incident. Despite the setback, the company remains committed to accelerating its technology transformation and recovery efforts. CEO Stuart Machin emphasized resilience and customer support. The incident follows an increasing trend of cyberattacks targeting UK businesses, which have also affected Co-op, Harrods, and the British Library. Meanwhile, M&S reported strong financial results prior to the attack, including a 22.2% rise in adjusted pretax profit and a 6.1% sales increase, benefitting food and clothing segments. Competitors like Next, Tesco, and Sainsbury’s may gain from M&S's online setbacks.
7. <https://moneyweek.com/personal-finance/marks-and-spencer-online-order-problems> - Following a cyberattack on Marks & Spencer (M&S) over Easter weekend, the retailer’s online services have been disrupted since 25 April 2025. M&S has announced that customers will not be able to place online orders until at least July, although they can browse and place items in their baskets. The company estimates a £300 million hit to its 2025/26 operating profits and has been losing approximately £40 million in sales weekly due to the attack. Some customer data, including names, contact information, and order history, was stolen, but no payment or password details were compromised. M&S has contacted affected customers and is urging vigilance against phishing attempts. The cyberattack, reportedly carried out by a group called DragonForce, involved ransomware. The company has suspended its Sparks loyalty offers and is focusing on business recovery, assuring that its long-term growth plans remain unchanged. While M&S shares have dropped 4.9% year-to-date, analysts remain optimistic, highlighting robust performance in its food sector and suggesting potential for long-term investor gains once stability returns. Compensation has been offered to impacted customers in some cases.