# Marks & Spencer cyber attack exposes vulnerabilities in UK retail and food supply chains



In recent weeks, several high-profile UK retailers, including Marks & Spencer (M&S), the Co-op, and Harrods, have endured significant turmoil following cyber attacks that severely disrupted their operations. M&S faced immediate challenges such as halted online orders, empty store shelves, and the inability of staff to process payments other than cash. Alarmingly, the attack has also resulted in compromised customer data, indicating a broader vulnerability across the retail sector.

M&S's decision to temporarily pause its online recruitment reflects the ongoing implications of this cyber incident. Over 200 job listings were removed from its website, as the company stated, “Sorry you can't search or apply for roles right now, we're working hard to be back online as soon as possible.” This disruption underscores the pervasive impact of cybercrime, not just on retail operations but also on employment opportunities within these establishments.

Adding to the context, the attack is believed to be orchestrated by the group known as Scattered Spider, which has a notorious record of targeting large corporations to extort and steal sensitive information. This case has led to significant disruptions, not just for M&S, but also in the broader landscape of the UK food supply chain, where experts are now calling for enhanced cybersecurity measures, such as phishing-resistant multi-factor authentication. The National Cyber Security Centre (NCSC) is actively involved in investigating the incidents and has urged UK businesses to take these threats seriously, highlighting the urgent need for improved identity security and rigorous third-party risk management.

In Spain and Portugal, recent power cuts have similarly brought critical infrastructure to a standstill, affecting various sectors from public transport to hospitality, with tourists stranded at airports without viable options to access their funds. Such operational failures serve as a vital reminder that not all disruptions are under the control of individual businesses, but they nonetheless impact customer experiences and expectations.

Additionally, a technical glitch affecting over 1.2 million people during the recent February payday further exemplifies the challenges consumers face when banking systems fail. In these scenarios, the right to compensation can be complex; individuals should be aware that claims can be made for both direct losses—such as being unable to pay essential bills—and consequential losses—like missed job opportunities due to financial limitations.

If a technical failure occurs, consumers are advised to monitor official news sources for updates on breaches or extended service outages. M&S and the Co-op have been relatively forthcoming in acknowledging the breach of data, which is commendable; however, companies often delay personal notifications, opting instead for vague public statements. GDPR regulations stipulate that businesses must inform individuals about data breaches likely to “adversely affect individuals’ rights and freedoms,” though this determination often becomes a point of contention.

To mitigate risks, individuals should adopt proactive measures such as changing passwords regularly and utilising password management tools, alongside enabling two-step authentication and biometric security options. These actions provide an additional layer of security, reducing the likelihood of falling victim to cyber threats.

For those unable to access vital banking services, it is crucial to understand the nuances of seeking compensation. Individuals experiencing direct financial impact from bank failures should document their experiences meticulously, as this helps in substantiating claims for distress and inconvenience. While compensation for consequential losses may be more challenging to obtain, well-documented instances of extenuating costs can enhance the prospect of a favourable resolution.

As the retail sector grapples with the fallout from these cyber attacks, it becomes increasingly evident that enhancing cybersecurity protocols is not merely advisable but essential for safeguarding not only corporate interests but also consumer rights and public trust. In a world where technology underpins almost every facet of daily life, the push for better security measures has never been clearer.

## Reference Map:

* Paragraph 1 – [[1]](https://www.mirror.co.uk/money/ms-cyber-attack-what-business-35277555), [[6]](https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos)
* Paragraph 2 – [[1]](https://www.mirror.co.uk/money/ms-cyber-attack-what-business-35277555), [[2]](https://news.sky.com/story/m-s-pauses-recruitment-amid-ongoing-cyber-attack-13359330)
* Paragraph 3 – [[4]](https://www.shieldsgazette.com/business/ms-marks-and-spencer-scattered-spider-online-cyber-attack-uk-shopping-5110689), [[5]](https://securitybrief.co.uk/story/cyber-attack-on-m-s-exposes-uk-food-supply-chain-risks)
* Paragraph 4 – [[1]](https://www.mirror.co.uk/money/ms-cyber-attack-what-business-35277555), [[6]](https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos)
* Paragraph 5 – [[1]](https://www.mirror.co.uk/money/ms-cyber-attack-what-business-35277555), [[3]](https://www.aljazeera.com/news/2025/5/2/harrods-ms-hit-by-cyberattack-what-happened-whos-behind-it)
* Paragraph 6 – [[4]](https://www.shieldsgazette.com/business/ms-marks-and-spencer-scattered-spider-online-cyber-attack-uk-shopping-5110689), [[5]](https://securitybrief.co.uk/story/cyber-attack-on-m-s-exposes-uk-food-supply-chain-risks)
* Paragraph 7 – [[1]](https://www.mirror.co.uk/money/ms-cyber-attack-what-business-35277555), [[5]](https://securitybrief.co.uk/story/cyber-attack-on-m-s-exposes-uk-food-supply-chain-risks)
* Paragraph 8 – [[3]](https://www.aljazeera.com/news/2025/5/2/harrods-ms-hit-by-cyberattack-what-happened-whos-behind-it), [[6]](https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos)
* Paragraph 9 – [[1]](https://www.mirror.co.uk/money/ms-cyber-attack-what-business-35277555), [[3]](https://www.aljazeera.com/news/2025/5/2/harrods-ms-hit-by-cyberattack-what-happened-whos-behind-it)

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

## Bibliography

1. <https://www.mirror.co.uk/money/ms-cyber-attack-what-business-35277555> - Please view link - unable to able to access data
2. <https://news.sky.com/story/m-s-pauses-recruitment-amid-ongoing-cyber-attack-13359330> - Marks & Spencer (M&S) has halted all online job postings due to an ongoing cyber attack. The company removed over 200 job listings from its website, stating, "Sorry you can't search or apply for roles right now, we're working hard to be back online as soon as possible." This action reflects the broader impact of the cyber incident on M&S's operations. ([news.sky.com](https://news.sky.com/story/m-s-pauses-recruitment-amid-ongoing-cyber-attack-13359330?utm_source=openai))
3. <https://www.aljazeera.com/news/2025/5/2/harrods-ms-hit-by-cyberattack-what-happened-whos-behind-it> - Both M&S and Harrods have been targeted by cyber attacks. M&S suspended online orders and paused recruitment, while Harrods restricted internet access as a precaution. The National Cyber Security Centre (NCSC) is investigating, urging UK businesses to enhance cybersecurity measures. ([aljazeera.com](https://www.aljazeera.com/news/2025/5/2/harrods-ms-hit-by-cyberattack-what-happened-whos-behind-it?utm_source=openai))
4. <https://www.shieldsgazette.com/business/ms-marks-and-spencer-scattered-spider-online-cyber-attack-uk-shopping-5110689> - The cyber attack on M&S is believed to be orchestrated by the hacking group Scattered Spider, also known as Octo Tempest. This group is notorious for targeting large companies and stealing their data. The attack has led to significant disruptions in M&S's services and operations. ([shieldsgazette.com](https://www.shieldsgazette.com/business/ms-marks-and-spencer-scattered-spider-online-cyber-attack-uk-shopping-5110689?utm_source=openai))
5. <https://securitybrief.co.uk/story/cyber-attack-on-m-s-exposes-uk-food-supply-chain-risks> - The M&S cyber attack has exposed vulnerabilities in the UK's food supply chain. Experts emphasize the need for organizations to focus on identity security and third-party risk, recommending measures like deploying phishing-resistant multi-factor authentication and restricting administrative access. ([securitybrief.co.uk](https://securitybrief.co.uk/story/cyber-attack-on-m-s-exposes-uk-food-supply-chain-risks?utm_source=openai))
6. <https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos> - The M&S cyber attack has led to significant operational disruptions, including empty shelves in stores and halted online orders. The incident has resulted in a market value loss of over £650 million for M&S. The National Cyber Security Centre (NCSC) is working with affected companies to address the issue. ([theguardian.com](https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos?utm_source=openai))
7. <https://www.itv.com/news/2025-05-01/dragonforce-the-software-cyber-security-experts-believe-was-used-to-hit-m-and-s> - Cybersecurity experts believe that the ransomware used in the M&S cyber attack is called DragonForce. The attack has led to significant disruptions in M&S's services, including halted online orders and issues with contactless payments. ([itv.com](https://www.itv.com/news/2025-05-01/dragonforce-the-software-cyber-security-experts-believe-was-used-to-hit-m-and-s?utm_source=openai))