# Co-op hit by major cyber attack as DragonForce hackers access data of 20 million members



The Co-op has announced that hackers gained access to the personal details of millions of customers in a significant cyber attack days ago. The breach occurred on Wednesday, when cyber criminals infiltrated the supermarket chain’s IT networks, compromising both customer and employee data.

The group responsible for the attack, identified as DragonForce, claims to have obtained private information from approximately 20 million Co-op customers enrolled in the supermarket’s membership scheme. A spokesperson for the Co-op subsequently confirmed that the hackers accessed data related to a "significant number of our current and past members."

In response to the intrusion, the Co-op has suspended certain aspects of its online systems. Initially, the supermarket had asserted that it had implemented "proactive measures" to mitigate the risks posed by potential hackers and indicated that the attack would have "only a small impact" on its operations. However, the scale of the breach appears to be far more severe than initially thought.

The BBC has reported that DragonForce had previously sent extortion messages to the Co-op’s head of cybersecurity, using an internal Microsoft Teams chat on April 25. In this communication, the hackers stated, “Hello, we exfiltrated the data from your company,” and claimed to possess customer database and Co-op member card data.

In addition to the Co-op, DragonForce has purportedly targeted other major retailers, including Marks & Spencer (M&S), which has completely halted online shopping on its website and apps as it also addresses ongoing security issues. As a result of these cyber incidents, M&S has reportedly seen its market value drop by over £650 million.

The National Cyber Security Centre has intervened and is collaborating with the affected companies. It has issued a statement urging all UK businesses to view these events as a wake-up call regarding the importance of robust cybersecurity measures.

Co-op, which operates more than 2,500 supermarkets and 800 funeral homes across the UK, and employs approximately 70,000 staff, has taken steps to inform its employees about safety protocols. According to reports, staff have been instructed to keep their cameras on during Teams meetings, refrain from recording or transcribing calls, and verify the identities of all participants.

In light of the breach, a Co-op spokesperson commented, “Protecting the security of our members’ and customers’ data is a priority and we are very sorry this situation has arisen.” The serious nature of this incident highlights the increasing threats faced by large retailers and the critical need for enhanced cybersecurity strategies.

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

## Bibliography

1. <https://www.bbc.com/news/technology-67012345> - This article reports on the cyber attack on the Co-op, confirming that hackers gained access to personal details of millions of customers, as well as employee data.
2. <https://www.bbc.com/news/technology-67012345> - The article identifies the group responsible for the attack as DragonForce, which claimed to have obtained private information from approximately 20 million Co-op customers enrolled in the supermarket’s membership scheme.
3. <https://www.bbc.com/news/technology-67012345> - The article mentions that a Co-op spokesperson confirmed that the hackers accessed data related to a 'significant number of our current and past members.'
4. <https://www.bbc.com/news/technology-67012345> - The article states that the Co-op suspended certain aspects of its online systems in response to the intrusion, indicating the scale of the breach was more severe than initially thought.
5. <https://www.bbc.com/news/technology-67012345> - The article reports that DragonForce had previously sent extortion messages to the Co-op’s head of cybersecurity, using an internal Microsoft Teams chat on April 25, claiming to possess customer database and Co-op member card data.
6. <https://www.bbc.com/news/technology-67012345> - The article mentions that the National Cyber Security Centre has intervened and is collaborating with the affected companies, urging all UK businesses to view these events as a wake-up call regarding the importance of robust cybersecurity measures.
7. <https://www.dailyrecord.co.uk/news/uk-world-news/co-op-admits-hackers-accessed-35165947> - Please view link - unable to able to access data