# The Co-operative Group halts parts of its IT network after attempted cyberattack



The Co-operative Group has been compelled to shut down parts of its IT network following an attempted cyberattack, affecting its operations. The organisation, which operates over 2,000 food shops across the United Kingdom as well as providing insurance and funeral services, informed staff via a letter that it had taken precautionary measures to protect its systems.

In the communication, the Co-op acknowledged an attempt by a hacker to gain "unauthorised access" to its IT infrastructure. As a security measure, it stated that it had "pre-emptively withdrawn access to some systems" to safeguard against any potential breach.

According to a report by The Guardian, this enforced IT shutdown resulted in the closure of virtual desktops used by staff, disrupting several operational functions such as updating stock levels. The incident, occurring amid a series of cyber threats targeting retail businesses, recalls a similar attack recently experienced by Marks & Spencer. That attack, disclosed publicly last week, also caused significant disruptions, including preventing customers from placing online orders and leaving some food stores with shortages on their shelves.

The Co-op's actions underline the increasing cybersecurity challenges faced by large retail and service providers in the UK. While the organisation has not disclosed further technical specifics about the attack or identified the perpetrators, the proactive response highlights the importance placed on preventing unauthorised access and minimising operational impact.

The Times is reporting on this development as part of ongoing coverage of cyber threats affecting the retail sector.

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

## Bibliography

1. <https://www.reuters.com/world/uk/britains-co-op-is-latest-retailer-to-be-hit-by-cyber-attack-2025-04-30/> - This Reuters article reports on the Co-op Group's cyberattack, detailing the attempted breach and the company's precautionary shutdown of certain IT systems to protect its infrastructure.
2. <https://www.reuters.com/business/retail-consumer/britains-ms-pauses-some-online-orders-after-cyber-incident-2025-04-25/> - This Reuters report discusses Marks & Spencer's cyber incident, highlighting the temporary halt of online orders and the impact on food availability in some stores.
3. <https://www.ft.com/content/1d46953a-5f2d-4395-85b9-af337a4747db> - The Financial Times article provides insights into the financial impact of the cyberattack on Marks & Spencer, noting a significant drop in the retailer's market valuation.
4. <https://www.reuters.com/technology/cybersecurity/ms-tells-warehouse-agency-staff-stay-home-cyber-incident-continues-2025-04-28/> - This Reuters piece details the operational disruptions at Marks & Spencer's distribution center due to the ongoing cyber incident, including instructions for agency staff to stay home.
5. <https://www.reuters.com/business/retail-consumer/britains-ms-says-cyber-attack-has-hit-food-availability-some-stores-2025-04-29/> - This Reuters article reports on the cyberattack affecting Marks & Spencer, leading to disruptions in food item availability in some stores and the temporary suspension of online orders.
6. <https://www.thenews.coop/cyberattack-knocks-out-systems-at-canadas-federated-co-op-stores/> - This Co-operative News article discusses a cyberattack on Canada's Federated Co-op stores, highlighting the operational challenges faced by the organization due to the IT disruption.
7. <https://www.thetimes.com/uk/crime/article/coop-it-shutdown-hack-attempt-x09pw2zg8?region=global> - Please view link - unable to able to access data