# Tyler Buchanan alleged as leader of Scattered Spider gang behind £20m UK retail cyberattacks



As cyber threats escalate, a "dangerous" hacking gang linked to significant breaches in the UK retail sector is drawing grave concern from law enforcement officials and cybersecurity experts. Tyler Buchanan, a 23-year-old from Dundee, has been identified as a suspected leader of the notorious group called Scattered Spider, which is allegedly responsible for serious attacks on various high-profile brands, including Marks & Spencer (M&S) and others.

The FBI has named Buchanan as a pivotal figure within Scattered Spider, claiming his involvement in activities that culminate in a staggering £20 million bitcoin scam. Following a recent cyberattack on M&S, which resulted in the theft of some customer personal data but reportedly did not compromise payment details, the implications for the retail industry are worrying. M&S has faced operational disruptions since April 25, halting online orders and resulting in estimated losses of over £4 million per day, alongside a £1 billion drop in its market capitalisation.

Recent reports indicate that the gang, composed of approximately 1,000 individuals from both the UK and the US, employs tactics primarily based on social engineering. While many narratives characterise these criminals as highly sophisticated operators, experts argue that the group's reliance on basic techniques such as phishing and SIM swapping belies the more sensational images often propagated in the media. The glamorization of groups like Scattered Spider serves to inflate their status, potentially creating an appealing narrative for young, impressionable recruits.

Buchanan's alleged criminal activity took a dangerous turn in February 2023 when a raid at his family home reportedly forced him to flee Dundee. This incident sparked concern that gang warfare within the online realm could spill into physical confrontations, as evidenced by the arrival of a masked group at his mother's residence demanding passwords.

In light of these developments, Graeme Pearson, a former head of the Scottish Crime and Drug Enforcement Agency, has warned that such hacking collectives pose a substantial threat to the economy. He emphasised that while these individuals may not be overtly violent, the damage they inflict is profound, leading to diminished trust in financial and retail systems. The potential for organised crime to latch onto these activities adds an additional layer of urgency to the issue.

Cybersecurity experts, including Professor Bill Buchanan of Edinburgh Napier University, echo these concerns, highlighting the potential for large-scale attacks on key infrastructure in Scotland. While it is noted that many organisations have invested significantly in cybersecurity measures, gaps still remain, especially within public-sector services where adequate protective measures are often lacking.

These attacks have raised alarm bells throughout the UK, prompting calls from government officials for businesses to reassess their cybersecurity protocols. In the wake of multiple breaches, including attacks on the Co-op and Harrods, the British government is preparing to introduce a Cyber Security Bill aimed at enhancing national defence against such threats. The Cabinet Office Minister has labelled the recent incidents a "wake-up call," urging all organisations to treat cybersecurity as an "absolute priority."

The retail sector's vulnerabilities are exacerbated by outdated IT systems and the vast amounts of sensitive consumer data held by these companies. As businesses increasingly grapple with rising cyber insurance premiums — some by as much as 10% — the broader implications for investor confidence and market stability cannot be overlooked. Marks & Spencer's temporary inability to process online orders demonstrates the immediate economic repercussions of a well-executed cyberattack.

Experts recommend that proactive measures, including the adoption of encryption for sensitive data and enhanced continuous monitoring systems, must be implemented to counteract the growing threat landscape. Improving public awareness and instilling more robust cybersecurity practices can pave the way for resilience against future attacks. The urgency of addressing these vulnerabilities is clear, as the ever-evolving tactics employed by groups like Scattered Spider pose a formidable challenge both for businesses and the safety of consumers’ sensitive information.

As the threat of cybercrime continues to loom large, the interplay between technology and criminal activity demands a response that transcends mere rhetoric. Moving forward, a collaborative approach involving academia, law enforcement, and the private sector will be essential to bolster defences and address the underlying vulnerabilities that have been exploited in these devastating attacks.

### Reference Map

1. Paragraphs 1, 2, 3, 4
2. Paragraph 5
3. Paragraph 6
4. Paragraph 7
5. Paragraph 8
6. Paragraph 9
7. Paragraph 10
8. Paragraph 11
9. Paragraph 12

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

## Bibliography

1. <https://www.dailyrecord.co.uk/news/scottish-news/dangerous-hacking-gang-led-young-35219101> - Please view link - unable to able to access data
2. <https://www.reuters.com/business/retail-consumer/uks-ms-says-customer-information-was-taken-cyber-attack-2025-05-13/> - Marks & Spencer (M&S) confirmed a cyber attack that compromised some customer personal data, though no usable payment information or passwords were taken. The attack, widely identified as a ransomware incident, has significantly disrupted M&S's online operations, halting online orders since April 25. Despite the breach, M&S emphasized there is no evidence the stolen data has been shared and reassured customers that no action is required from them at this time. The company is working with cybersecurity experts, law enforcement, and government agencies to restore operations and secure its systems. ([reuters.com](https://www.reuters.com/business/retail-consumer/uks-ms-says-customer-information-was-taken-cyber-attack-2025-05-13/?utm_source=openai))
3. <https://www.ft.com/content/55221f2d-00b3-4856-9158-dfdd0263bd0c> - The article critiques the glamorization of cybercriminal groups like "Scattered Spider." Despite recent disruptions to UK retailers such as Marks and Spencer, the Co-op, and Harrods speculated to be linked to this group, its actual methods rely more on basic social engineering tactics than advanced technical skills. These include phishing, SIM swapping, and exploiting weak verification processes to gain unauthorized access. The cybersecurity industry, aiming to market its products, often assigns dramatic names to such groups—Scattered Spider being coined by CrowdStrike—which helps sensationalize their impact and sells fear-based solutions. These names can unintentionally bolster the criminals' status and recruitment appeal, especially among young offenders seeking prestige. The article argues for a shift away from inflated narratives toward a mature approach to cybersecurity, emphasizing early intervention, better detection, law enforcement training, and international cooperation. It stresses that addressing cybercrime effectively requires both reducing vulnerabilities and increasing the likelihood of prosecution for offenders. ([ft.com](https://www.ft.com/content/55221f2d-00b3-4856-9158-dfdd0263bd0c?utm_source=openai))
4. <https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1> - UK retailers are facing significant cyber insurance premium increases, up to 10%, following high-profile cyber attacks on major chains such as Marks and Spencer (M&S), Harrods, and the Co-op. These attacks are prompting insurers to reassess cyber risk in the retail sector, which had enjoyed falling rates in 2023 and 2024. Experts warn cyber security scrutiny will intensify and some insurers may withdraw from the retail market. M&S may claim tens of millions of pounds for business interruption, after losing over £40 million in online sales during a lengthy system outage. The Co-op confirmed a data breach affecting numerous customers. The sector is particularly vulnerable due to large amounts of consumer data and outdated IT systems. Tesco acknowledged ongoing cyber threat preparedness in its annual report, citing crisis simulations involving ransomware. Insurance might cover not only ransomware payments but also costs associated with crisis response. However, insurers face challenges if attackers are linked to sanctioned entities. The UK’s cyber security agency has also issued warnings about attackers impersonating IT help desks in sophisticated social engineering scams. Brokers urge businesses to secure cyber insurance now before premiums rise further. ([ft.com](https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1?utm_source=openai))
5. <https://moneyweek.com/personal-finance/marks-and-spencer-online-order-problems> - Marks & Spencer (M&S) continues to face serious operational disruptions following a cyberattack that occurred over the Easter weekend. Online orders through its website, app, and phone have been suspended since April 25, with no confirmed restart date. The attack compromised some customer data, including names, contact information, and order histories, though no payment details or passwords were exposed. As a security measure, customers will be prompted to reset their passwords upon their next login. Services including Sparks loyalty offers have been paused, and in-store stock availability remains inconsistent, as illustrated by images of empty shelves shared by shoppers online. The cyberattack has severely impacted M&S financially, with an estimated £4 million a day in lost online sales and an 18% drop in share value, erasing over £1 billion in market capitalization. While some affected customers have been compensated with gift cards, broader investor confidence is shaken due to limited communication from M&S. The ransomware group “DragonForce” has claimed responsibility for the breach. Despite these challenges, M&S's core food business and partnerships like Ocado remain unaffected, providing a silver lining during this crisis. The company is actively working to resolve the issue though no timeline has been confirmed. ([moneyweek.com](https://moneyweek.com/personal-finance/marks-and-spencer-online-order-problems?utm_source=openai))
6. <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))
7. <https://www.reuters.com/business/retail-consumer/britain-warn-companies-cyber-security-must-be-absolute-priority-2025-05-02/> - The British government is set to urge all UK businesses to prioritize cyber security following recent cyberattacks on major retailers Marks & Spencer (M&S), the Co-op Group, and Harrods. Cabinet Office Minister Pat McFadden, in coordination with national security officials and Richard Horne, CEO of the National Cyber Security Centre, outlined governmental support for affected companies. At the upcoming CyberUK conference in Manchester, McFadden will stress the need for heightened cyber precautions, describing the attacks as a "wake-up call" and advocating for cyber security to be treated as an "absolute priority." New measures, including the Cyber Security Bill, are being introduced to strengthen national defense. M&S experienced significant disruption on April 25 due to a suspected ransomware attack by the group "Scattered Spider," which affected their online and contactless services. This incident follows a growing trend of cyberattacks causing extensive financial and operational damage across UK industries. ([reuters.com](https://www.reuters.com/business/retail-consumer/britain-warn-companies-cyber-security-must-be-absolute-priority-2025-05-02/?utm_source=openai))