

UK to Ban Public Sector Ransom Payments in Crackdown on Cybercrime

July 23, 2025

— Categories: Defence & Security



The UK government is preparing legislation to ban public sector organisations from paying ransoms to cybercriminals, in a significant move to reduce the financial appeal of ransomware attacks. The proposed law is part of a wider cybersecurity strategy aimed at protecting national infrastructure and discouraging criminal targeting of state services.

Under the new rules, public sector bodies, including hospitals, councils, schools, and national infrastructure operators, would be legally prohibited from making ransom payments in the event of a cyberattack. The government says the approach will remove the incentive for hackers to target critical services by cutting off their revenue stream.

Security Minister Dan Jarvis said the measures are designed to send a clear message that the UK will not fund criminal activity. “This is about defending our institutions, protecting public funds, and standing firm against extortion,” he stated. Jarvis added that the reforms are intended to strengthen the UK’s resilience against an increasingly aggressive and sophisticated threat landscape.

The proposed legislation would also introduce a mandatory notification system for private firms that intend to pay ransoms. Companies would be required to inform the National Crime Agency in advance, allowing authorities to assess the legality of the payment and whether it breaches any sanctions or national security concerns. In cases involving known terrorist networks or sanctioned entities, payment could be blocked outright.

The government is also exploring the introduction of a mandatory reporting system for ransomware incidents to improve data gathering and enhance law enforcement’s ability to trace and dismantle criminal operations.

Cybersecurity experts have largely welcomed the move. Some have described it as one of the most decisive global steps to undermine ransomware as a business model. Statistics from the past year indicate that while ransomware attacks have increased, total ransom payments

have fallen, suggesting that victim refusal is beginning to impact the profitability of these operations.

However, critics caution that banning ransom payments could have unintended effects, including hackers shifting focus to the private sector or smaller organisations with fewer resources. The success of the policy will hinge on robust cyber defences, early threat detection, and rapid response capabilities across public services.

Still, ministers believe the long-term benefit of eroding ransomware economics outweighs the short-term risk. As digital threats continue to evolve, the UK appears determined to harden its defences and send a clear warning to would-be attackers that extortion will no longer pay.