The downfall of the teenage hacker who crippled TfL from his bedroom

telegraph.co.uk/news/2026/07/17/downfall-teenage-hacker-crippled-tfl-bedroom

Rosa Silverman July 17, 2026

Now jailed for five years, Thalha Jubair's 16-hour cyberattack cost the transport network £29m before a simple mistake caught up with him

Thalha Jubair, now 20, has been sentenced to five-and-a-half years in prison after pleading guilty to a cyberattack on TfL

In his bedroom in a 22-storey tower block in east London, Thalha Jubair entered another world. As a teenager, he was, like so many, a gamer. But his skills led him into a dark sphere of cyber criminality, and his actions would end up causing serious financial harm and land him in prison.

This week, the 20-year-old was sentenced to five-and-a-half years in jail after pleading guilty to a cyberattack on Transport for London (TfL). Along with Owen Flowers, 18, from Walsall, he conspired in 2024 to hack the transport operator's systems, costing it £29m.

Only these two young men knew their ultimate aim, but in practice, their escapades compromised the data of some 10 million passengers and made 148 TfL systems inoperable. Dial-a-ride services used by disabled Londoners were heavily disrupted. Indeed, what they brought about was disruption to a "vital part of the UK's critical

infrastructure", the National Crime Agency (NCA) said, after spending almost two years working with the CPS and police to bring them to justice.

Jubair and his accomplice, Owen Flowers (pictured), compromised the data of some 10 million TfL passengers Credit: BBC

After being sentenced, other high-profile hackers have, in the past, used their considerable technological skills to help rather than thwart authorities. Whether Jubair might ever join their ranks, though, is a subject of contention among the experts that *The Telegraph* spoke to.

Jubair's hacking journey began high above the streets of the city in which thousands of transport users would be inconvenienced by what he did. Here, at the Tower Hamlets council flat of his loving parents, he honed his technological skills and fell into what his lawyer described as an "isolated life online".

Jubair was only four years old when he received his first smartphone, said Paul Keleher KC. By the age of six or seven, he had his first laptop, and by nine or 10, he was writing computer programmes. By 13, he had been introduced to hacking by older criminals online "who recognised his potential", Keleher said.

Jubair was "like a 21st-century Oliver Twist", his barrister added. "If you can find a child like Jubair, you can use his nimble skills for hacking for profit."

Diagnosed with autism spectrum disorder, Jubair was "isolated and bullied at school," Woolwich Crown Court heard. He also has depression and a severe mood disorder. His mother gave up her job working with children who have special needs to care for him full-time. His father, meanwhile, works in the care sector. His life could have gone either way.

Despite his many challenges, Jubair attended a local school in east London, passed a number of GCSEs and had even applied to colleges. But the path he had already embarked on took him into a murky online underworld at a young age.

Jubair's barrister called him a '21st-century Oliver Twist' Credit: BBC

On video game platforms, he began by stealing fellow players' usernames, *London Centric*, a news website, reported. Jubair is believed to have been just 14 when he graduated from gaming into what is known as SIM-swapping. This trick enables cyber criminals to collect personal details shared by others on social media and use them to hijack their mobile numbers. It means authentication codes can then be sent directly to them.

By 2022, Jubair, then aged 16, was allegedly helping run a channel on Telegram, the encrypted messaging app, in which SIM-swapping services were sold to other hackers, *London Centric* reported.

The news website, which spent more than a year investigating him, says the teenage hackers involved in this operation were trying to get hold of other people's cryptocurrency, which they realised they could do by taking control of the person's phone number and resetting their password. They reportedly did so by calling up the relevant telecoms firm and talking the company into transferring a target's phone number to a phone they had in their possession.

Eventually, Jubair joined, and became a leading member of, a hacking group called Scattered Spider. The group is believed to be responsible for hundreds of cyber attacks between 2022 and 2025. It has posed the most significant cybercrime threat to the UK in recent years, said Paul Foster, head of the NCA's cybercrime unit.

His TfL hack with Flowers was not even the first time his actions led him into the arms of the law. He had been convicted of 22 offences as a teenager, among them 13 counts of fraud, two of unauthorised access to a computer and one of blackmail. In a youth court, he was convicted of stalking two young women and hacking into a City of London police server.

He was 18 when he and Flowers, then 17, hacked into London's transport authority at 5pm on Aug 31 2024. Their ensuing 16-hour cyberattack was streamed online, the court heard.

Jubair now faces an extradition battle with the US, where he is accused by federal prosecutors of masterminding other hacks. In fact, US prosecutors have reportedly attributed to Jubair and his associates at least $115m (£86m) in ransom payments. They also told the British courts that more than £200m in total had passed through cryptocurrency wallets controlled by Jubair in his teens.

Before being sentenced, Jubair had been convicted of 22 offences as a teenager, among them 13 counts of fraud Credit: Elizabeth Cook/PA

Could his savant-like technological skills have been channelled into something constructive? Rob Pritchard, a cybersecurity expert, is sceptical. "There's a tendency to think of these people as people who could be redirected," he says. "[But] it's not like these technological skills are so hard to come by."

Still, some of the higher-profile anonymous activist hackers from 20 years ago have since moved into security research, he notes. "So if you're technologically adept, that route is

there. But it’s there for you anyway. There are not that many teens who are doing [this kind of hacking], so it’s not like we’re missing out on some untapped resources.”

The danger comes when young people with these abilities are left without boundaries or a legitimate outlet, cautions Kevin Walker, a specialist at Black Swan Cyber Security Solutions who has worked in schools for more than 20 years.

“With the right nurturing, the same curiosity that asks, ‘Can I get into this system?’ can become the professional instinct that asks, ‘How do we stop somebody else getting in?’” he says. “The difference is permission, ethics and opportunity. Cybersecurity needs people who think outside the box, pull systems apart, notice what others miss and refuse to accept that something is secure simply because the vendor says it is. These are exactly the qualities we need to protect our schools, hospitals, businesses and public services.”

Online hacking communities often reward bravado and make an attack feel like a game, he says. But most young people who experiment with technology are not “inherently bad”, he believes. “Many are curious, highly focused and determined to understand how things work. Some are neurodivergent and may see patterns or weaknesses that other people miss. These are valuable qualities in cybersecurity, but the challenge is to give young people clear ethical boundaries, and somewhere safe and legal to test their abilities before an online mistake turns into a criminal record.”

In Jubair’s case, it’s too late for this. The behaviour his barrister described as “seeking validation using his technological skills” ultimately saw him arrested at his home address on Sept 16 last year. He had reportedly made a basic error by ordering a takeaway using food delivery gift vouchers bought with a cryptocurrency wallet that was hosted on the same server he and other hackers had allegedly used to store tens of millions of dollars in Bitcoin paid in ransoms by US firms.

His and Flowers’ case, says the NCA, is the largest cybercrime prosecution ever brought before the UK courts.

The threat they posed has been neutralised – although the court heard that even while behind bars awaiting trial, Jubair and Flowers were both found with contraband phones. Recovered messages show them continuing to talk about and coordinate future cyberattacks.

And, of course, there will be others out there, too. The ongoing challenge for the authorities is disrupting their actions before they can disrupt people’s lives.

From the Editor PM

Catch up on the day's news and ease into the evening with our best features and recommendations, in your inbox every weekday afternoon

WAS · IS · & · WILL · BE
LONDON
1855