# Dundee man faces trial for alleged cyber attacks on global institutions



A Dundee man, Coray Tierney, is facing trial later this year on charges related to cyber attacks against several high-profile organisations, including the Bank of Israel and the FBI. The 23-year-old from Yarrow Terrace has been accused of violating the Computer Misuse Act through denial of service attacks targeting entities such as HSBC, Malwarebytes, and Epic Games Inc, the creators of the popular game Fortnite. These alleged cyber incidents reportedly took place between December 2021 and March 2023.

At a recent hearing at Dundee Sheriff Court, it was announced that Tierney's trial is set to proceed on September 8, pending an outstanding cybercrime report. His solicitor, Jim Caird, expressed the significant personal impact of the case on Tierney, stating, “It’s been an enormous inconvenience for Mr Tierney,” who has appeared in court six times regarding the matter. Caird highlighted that the seizure of Tierney's computer by the police has prevented him from engaging in his interest in video gaming. Currently, Tierney is on disability benefit and has not been working.

Sheriff Grant McCulloch remarked on the seriousness of the allegations, particularly given the involvement of foreign states and institutions, indicating that such cases cannot be dismissed lightly.

In a separate case, Jay Dixon, also from Dundee, pled guilty to endangering the life of a newborn baby. The 23-year-old admitted to two incidents of domestic abuse towards partners, alongside charges of neglect and serious assault against the infant, who was less than a month old.

In another matter, Grant Young was sentenced on his 40th birthday to a maximum of 12 months in prison after being found guilty of assaulting a woman in her home in Fife. The assault, which involved multiple punches to the head, left the victim "bloodied." Sherif Kirsta Johnston noted Young’s previous record of violent behaviour, emphasising a disturbing pattern of domestic violence. The court also revealed Young's history of using offensive language and making derogatory comments towards other women.

In Dundee, a teenager known as Cody Chambers received a sentence for an assault that left another youth with a permanent scar after striking him with a hammer during a children’s football game.

David Tracey, aged 37, was sentenced to nine months in prison after admitting to breaking into a Co-op store in March. Along with an accomplice, he stole goods valued at £666.01. Tracey’s conduct escalated when he later confronted an employee at a Tesco Express, resulting in charges of violence and aggressive behaviour.

Russel Gray, a 47-year-old man, received a sentence of 25 months and two weeks for his involvement in a robbery in Montrose. The court heard that he, along with two accomplices, lured a man into a trap under the pretense of soliciting help. The group assaulted the victim and made off with personal belongings, including a mobile phone and cash.

In another court ruling, Patrick Jess, a former president of the St Andrews Rifle Club, was placed under supervision after being convicted of multiple sexual assaults on female students. He has also been mandated to complete unpaid work as a punishment instead of serving prison time.

Lastly, serial fraudster Christopher Menmuir, 27, has been ordered to pay compensation to three victims following his conviction for defrauding individuals out of nearly £3,000. Menmuir, who had been facing personal difficulties, failed to deliver promised services and merchandise to his victims, leading to a fine and compensation order from Forfar Sheriff Court.

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

## Bibliography

1. <https://www.timesofisrael.com/israeli-british-man-in-court-for-cyber-attack-on-uk-banks/> - This article discusses Daniel Kaye, a dual Israeli-British citizen, who appeared in court after being extradited from Germany for allegedly launching cyber attacks against two of Britain’s best-known high-street banks and attempting to blackmail them. The attacks are estimated to have cost Lloyds £190,000 and Barclays around £146,000.
2. <https://www.bankinfosecurity.com/breach-roundup-fcc-proposes-cybersecurity-prog-for-schools-a-23602> - This article reports on a surge of data-wiping attacks in Israel, where hackers adapted the BiBi malware family to target both Linux and Windows systems. The attacks prompted the government's Cyber Emergency Response Team to issue identifiers for detection. The malware, linked by researchers at Palo Alto to an Iranian-backed APT group called Agonizing Serpens, erases data without encryption or ransom demands.
3. <https://www.calcalist.co.il/ctechnews/article/irk57fqxb> - This article highlights the surge in cyber assaults during the war, noting that the National Cyber Directorate identified 1,900 cyber incidents with potential for significant damage in the past year—a threefold increase compared to the previous year. Between October 7 and December 31, 2023, 3,380 cyberattacks were detected, 800 of which were classified as significant threats.
4. <https://www.shomrim.news/eng/irans-cyber-onslaught-from-data-heist-to-digital-warfare-in-israel> - This article discusses the cyber attacks attributed to Iranian-affiliated hacker groups, which infiltrated and shared sensitive data on the dark web and hacker forums. The leaks included personal information of Israeli citizens and soldiers, highlighting the vulnerabilities in Israel's cyber defenses.
5. <https://www.bankingriskandregulation.com/israels-cyber-iron-dome-protects-israeli-banks-from-cyberattack-onslaught/> - This article reports on Israel's 'Iron Dome' cyber defense system, which protected the country's banks from a significant onslaught of cyberattacks. Despite being the third most targeted sector since hostilities with Hamas began on October 7, the banking sector's resilience relied on a unique data-sharing collaboration between financial institutions and other sector-critical industries.
6. <https://www.jpost.com/israel-news/defense-news/article-751792> - This article discusses the persistent state of cyber warfare between the US, Israel, and adversaries such as China, Russia, Iran, North Korea, and Hezbollah. It highlights incidents like the false rocket-warning sirens activated in Jerusalem and Eilat on June 19, 2022, caused by a cyber attack attributed to Iran.
7. <https://www.thecourier.co.uk/fp/news/courts/5234503/friday-court-round-up-jailed-birthday/> - Please view link - unable to able to access data