

OpenVoiceNews India

Transparent. Unbiased. Yours.

Canadian Teen Sentenced in \$37M Bitcoin Theft, X Account Hacks

August 4, 2025

– Categories: Crypto



©CanadiansInternet

Download IPFS

A Canadian teenager has been sentenced for orchestrating a \$37 million Bitcoin theft and participating in a 2020 hacking spree that compromised several high-profile X (formerly Twitter) accounts. The conviction marks one of the largest cryptocurrency-related fraud cases in Canadian history.

Authorities revealed that the crimes were carried out using SIM swapping and social engineering techniques, allowing the teenager to take control of victims' phone numbers, intercept two-factor authentication codes, and gain unauthorized access to online accounts. The stolen cryptocurrency was valued at approximately \$37 million at the time of the theft.

The sentencing follows growing calls from cybersecurity experts for stronger laws and harsher penalties for SIM swapping offenses. On-chain investigator ZachXBT, known for tracking cryptocurrency scams and thefts, has repeatedly highlighted the ease with which attackers exploit mobile carrier vulnerabilities to execute such schemes.

The teen's role in the 2020 X hacking incident involved breaching several verified accounts, some belonging to well-known public figures, and posting fraudulent messages promoting cryptocurrency scams. Victims were tricked into sending Bitcoin to attacker-controlled wallets under the false promise of doubled returns.

Law enforcement agencies from multiple jurisdictions collaborated on the case, tracing stolen funds through blockchain analysis and working with cryptocurrency exchanges to freeze and recover a portion of the assets. Despite these efforts, a significant amount of the stolen Bitcoin remains unaccounted for.

Prosecutors emphasized that the case shows the risks posed by SIM swapping attacks, which have been linked to a rising number of cryptocurrency thefts and data breaches worldwide. They warned that individuals and businesses must adopt stronger security measures, including hardware-based authentication, to protect sensitive accounts.

The court also ordered the forfeiture of assets purchased with the stolen funds, including luxury items and high-value electronics. While the defendant's name has not been released due to Canadian youth offender protections, authorities confirmed that he will serve his sentence under a combination of youth custody and supervised release conditions.

SIM swapping involves convincing a mobile carrier to transfer a victim's phone number to a SIM card controlled by the attacker. Once the number is reassigned, the attacker can intercept calls and text messages, reset account passwords, and bypass security measures. Law enforcement agencies in North America have warned that the crime is increasingly targeting individuals with significant cryptocurrency holdings.

The conviction is expected to influence future cybercrime sentencing in Canada and may lead to legislative reforms aimed at curbing SIM swapping and related fraud schemes.