NT residents warned about crypto investment scams after one victim loses nearly $5m

Publication Date: 2024-02-06

Author: Josh Taylor

Section: Technology

Tags: Cybercrime, Internet, Northern Territory, Australian Competition and Consumer Commission (ACCC), news

Article URL: https://www.theguardian.com/technology/2024/feb/06/nt-cryptocurrency-investment-scams

Northern Territory police have warned that cryptocurrency investment scams are the biggest cause of financial harm to people there, with one resident losing nearly $5m to one scam. The massive loss was revealed in a submission to a federal inquiry on law enforcement capability around cybercrime. NT police said residents in the territory had suffered “significant losses” ranging from hundreds of thousands of dollars to the $4.98m lost by one person in 2022. “It is important to note that whilst for many victims who lose less than one hundred thousand dollars, the impact of such a loss is still very significant to the individual and their family,” NT police said in the submission. “It is extremely difficult for police to recover funds once they have been transferred to these fake investment companies. The level of personal harm through anguish and embarrassment leads to distinct under reporting of these events.” Banks, police, regulators and social media platforms are all struggling to stop the scourge of investment scams in the past few years. The scammers often use a fake celebrity endorsement in fake news articles to promote a scheme promising high returns only to result in people losing massive amounts of money. Australians lost a record $3.1bn to scams in 2022, up from $2bn in 2021. According to the latest data from 2023, there were losses reported to Scamwatch of $275m from investment scams. The billionaire Andrew Forrest and the Australian Competition and Consumer Commission have both launched legal action against Facebook’s parent company Meta, alleging it has not done enough to prevent scams. Banks have instituted features and rules designed to limit scams, including name matching for money going into another account and pauses on transfers of money to a new account as well as restrictions on some cryptocurrency exchanges. In its submission to the inquiry, the Australian federal police noted the growing crime phenomenon of large-scale human trafficking where victims are lured through fake job ads to online scam centres. The AFP said these trafficked workers are then used to perpetuate online fraud on a second set of victims, including through investment scams. The AFP also warned that many cybercrimes are becoming easier to launch, as malicious artificial intelligence tools used for ransomware attacks have lowered the bar for entry to attackers who might not have the skills or resources otherwise. The AFP said generative AI tools with names like FraudGPT and WormGPT, which offer a full suite of tools to launch malware or phishing attacks, began to emerge from the dark web and encrypted channels in July last year. Both the AFP and NT police said encrypted communications also presented a challenge for law enforcement investigations. The AFP said 94% of lawfully intercepted internet data by the AFP in 2021-2022 was “unintelligible due to the use of encryption” but said that new powers and warrants introduced under amendments to telecommunications and surveillance laws in 2018 and 2021, respectively, had allowed the AFP to develop “innovative ways to address this issue.”