He Used a $100 'WiFi Pineapple' to Steal Passwords From Airplane Passengers. Now He's Going to Prison.

An Australian man set up fake wireless networks at airports and on flights, tricking travelers into handing over their login credentials. The scheme went undetected for years.

The device that got Michael Clapsis arrested fits in a coat pocket and costs about $100 online.

It's called a WiFi Pineapple. Security professionals use it to test corporate networks for weaknesses. Clapsis, a 44-year-old from Australia used the device to steal the private photos of women he had never met.

Last week he was sentenced to seven years and four months in prison. He had pleaded guilty to 15 criminal charges, including unauthorized access to restricted data, stealing, and attempting to destroy evidence.

How He Orchestrated The WiFi Attacks – The Evil Twin Approach

The WiFi Pineapple is a small wireless device designed to mimic legitimate networks.

When Clapsis sat in an airport terminal or airplane seat, his device would listen for signals from nearby phones and laptops. These devices constantly search for familiar networks, broadcasting names like "Qantas Free WiFi" or "Melbourne Airport."

The moment his device detected such a request, it would create a matching network with the exact same name. The victim's phone or laptop would then connect automatically, believing it had found a trusted network.

Passengers who connected saw what looked like a standard login page. It asked them to sign in using their email or social media accounts.

Once they entered their credentials, the information was saved directly to Clapsis's laptop. The victims never got their free WiFi connection. Most probably assumed the system was just glitchy.

He Did The Wifi Attacks For Years

Australian Federal Police traced fraudulent WiFi pages to airports in Perth, Melbourne, and Adelaide. But he also did the attacks on planes.

But when investigators examined his seized laptop and phone, they found something worse than stolen passwords.

The devices contained thousands of intimate images and videos belonging to women. Clapsis had used the stolen credentials to access victims' social media

accounts and cloud storage. He monitored their private communications and downloaded their personal photos.

According to court documents, one victim was just 17 years old. Another was a police officer.

How He Eventually Got Caught

His Wifi attacks were detected in April 2024 during a domestic Qantas flight that he was taking.

Airline employees noticed a suspicious WiFi network on board the plane that appeared to copy the carrier's legitimate portal. They reported the suspicious WiFi to authorities who leaped into action while the plane was in the air.

When the flight landed at Perth Airport on April 19, investigators searched Clapsis's hand luggage. They found the WiFi Pineapple, a laptop, and a mobile phone.

A search warrant was later executed at his home in Palmyra, a suburb of Perth.

He Tried To Cover His Tracks

The day after investigators searched his home, Clapsis made a last minute attempt to destroy evidence on his devices.

He deleted 1,752 items from a cloud storage account. He also tried to remotely wipe his mobile phone, but the attempt failed and the data was never deleted.

Then he did something even more brazen and tried to spy on investigators. Between April 22 and 23, he used software tools to access his employer's laptop. His goal was to view confidential online meetings between his employer and the authorities about the investigation into his activities.

A Warning To Travelers About Free WiFi

AFP Commander Renee Colley urged travelers to be careful when connecting to free WiFi networks, especially at airports and other public spaces.

"A network that requests your personal details, such as an email or social media account, should be avoided," she said.

Colley recommended using a virtual private network, or VPN, when connecting to public WiFi. She also advised travelers to disable automatic WiFi connectivity on their devices and to select "forget network" after disconnecting from public hotspots.