Students turning to cyberfraud as huge phishing site infiltrated, police reveal

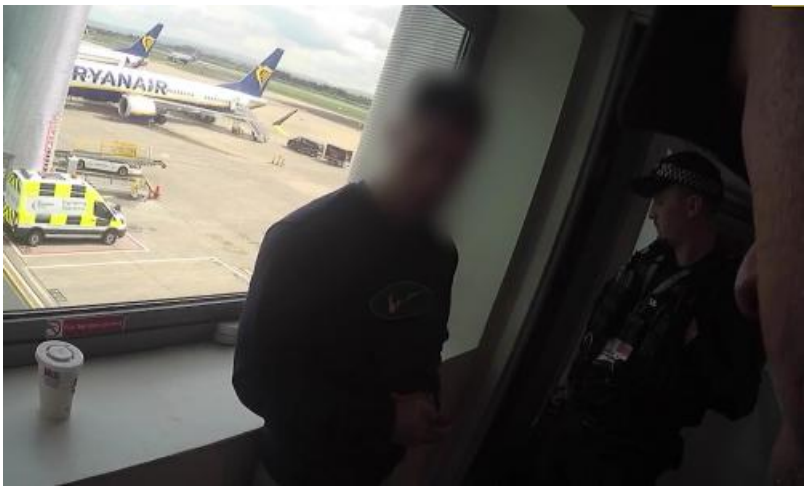
Publication Date: 2024-04-17

Author: Vikram Dodd

Section: Technology

Tags: Cybercrime, Internet, news

Article URL: https://www.theguardian.com/technology/2024/apr/18/students-turning-to-cyberfraud-as-huge-phishing-site-infiltrated-police-reveal



University students have turned to cyber fraud to boost their income, police have said, as they revealed they have infiltrated a huge phishing site on the dark web responsible for scamming tens of thousands of people. The site called LabHost was active since 2021 and was a cyber fraud superstore, allowing users to produce realistic-looking websites from household names such as the big banks, ensnaring victims around the world including 70,000 in the UK. Victims entered their sensitive details, some of which were used to steal money, but those behind the site also made money by selling details on the dark web for fraudsters to use. The Metropolitan police said that the main victims were aged 25 to 44 years, who conduct most of their lives online. Police believe they arrested one of the site's main alleged masterminds this week among 37 suspects detained across the UK and overseas. The Met said arrests were made at Manchester and Luton airports, and in Essex and London. Policing in the UK is under pressure to show it is successfully tackling the explosion in cyberfraud. The infiltration of the site is a relative drop in the ocean compared to the scale of the problem, but police hope to shatter the confidence of criminals who believe they can act with impunity, and plan to take down more cyberfraud sites. Fraud and cybercrime are seen as difficult to solve within policing amid battles for resources against other crime priorities such as protecting children and boosting what is widely seen as inadequate protection of women. For now, the Met is celebrating its success. In the UK, 25,000 victims have been contacted and arrests of the site's main users have taken place. However, some of those who used it will not be detained as their real identity remains unknown to investigators. LabHost amassed 480,000 debit or credit card numbers, 64,000 pin numbers and made £1m from membership fees alone from 2,000 people, which were up to £300 a month for membership, to be paid in cryptocurrency. It advertised itself as a "one-stop-shop for phishing". It offered a tutorial video on how to use the site to commit crime, similar to a video on how to use a new consumer product. The video said the software took five minutes to install, and offered "customer service" if there were any problems. It ended by wishing its criminal users to: "Stay safe and good spamming." DI Oliver Richter said five years ago a cyber fraudster would need technical skills, like being able to code. Now users are in their late-teens to late-20s. He said: "A lot of these users, they are younger, they're at university, they are very likely to go on to perhaps perfectly legitimate careers. "They see this, because it is so easy to do, as something that is anonymous. "They are entering into this, I think, not fully understanding the risks and potential outcomes." After the site was disrupted, 800 users received a message telling them that police "know who they are and what they've been doing". Police did not reveal how they gained entry to the inner workings of the site, which occurred in June 2022. Det Supt Helen Rance, head of the Met's cybercrime unit, said taking down the "incredibly slick" LabHost

was part of a Met effort to target those who “industrialised” crimes like fraud and 17 forces across the world were involved, as well as the private sector. She said: “We’ve managed to infiltrate this service so we could see those responsible for it and the scale of the operation.”