The National Investigation Agency (NIA) earlier this month arrested a 53 year old man named Abdul Rehman Abdul Jabbar Sheikh from Maharashtra's Mumbai for being an alleged terror funding conspirator in the Visakhapatnam espionage case that came to light last December in which 11 Indian Navy personnel allegedly leaked sensitive information to Pakistan's Inter-Services Intelligence (ISI) as part of a larger Pakistan-sponsored espionage network.

Sheikh's arrest has taken the number of arrests to 15, which include 11 naval personnel and Sheikh's wife, named Shaista Qaiser, who had been arrested earlier. Sheikh's arrest followed the arrest of another Mumbai-based businessman named Mohammed Haroon Haji Abdul Rehman Lakdawala last month. Haroon is accused of facilitating payments between Pakistan-based handlers and their alleged operatives in India, including the naval personnel.

The Visakhapatnam espionage case, codenamed Operation Dolphin's Nose, was cracked last December jointly by Andhra Pradesh Police, the naval intelligence, and a number of central agencies. Seven Indian Navy personnel and a hawala operator were then arrested for passing information to their handlers in Pakistan, who had recruited them through honey-trapping on social media. The case was subsequently transferred to NIA.

This is not an isolated incident but part of a string of incidents in which a number of men from the Indian security establishment have been recruited by Pakistan-based operatives through social media, particularly through honey-trapping in recent years.

In 2018, an engineer at the BrahMos missile's Nagpur unit named Nishant Agrawal was arrested for allegedly being a Pakistani operative after being honey-trapped. Agrawal's arrest closely followed the arrest of a Border Security Force personnel named Achutanand Mishra. Both Agrawal and Mishra were allegedly honey-trapped.

In June last year, it was found that one Facebook user had hacked into 98 social media accounts belonging to people in the Indian security establishment. This account, by the name of Sejal Kapoor, was also found linked to the Nishant Agrawal's case.

Image source: PTI

Mr Vinayak Dalmia, a cyber and national security expert, told The Kootneeti that the human element is central to most of these incidents. He said, “Most such incidents are generated as a result of phishing attacks and social engineering. Hackers build single-click or double-click exploits to do this. Therefore, most cyber security breaches are a result of human errors. It is only in zero-click exploits that a human in the loop is not needed.”

“Social engineering” refers to tactics in which you take information out of someone by exploiting their natural or emotional tendencies, such as honey-traps in which men are often targeted by operatives posing as women interested in them, luring them to share sensitive information in lieu of intimate conservations or sexual exchanges. This is often done through a “phishing attack” which refers to a nefarious program being installed into a system in guise of a harmless program to get information, such as a software for video chat with the “woman” that would actually steal information from the target’s system.

Therefore, most of the security breaches are enabled by the target itself. The onus of preventing the attack is on the security establishment and it has recognised this. The gravity of the situation has made the establishment set up dedicated units that constantly employ counter-measures to track attempts of honey-trapping and recruitment through

social media and trace the personnel falling for such networks.

The then Chief of the Army Staff General Bipin Rawat had raised the issue, saying personnel should be careful on social media and make friends there accordingly. The army also has a social media policy in place, guidelines pertaining to which are issued time to time. As more cases have appeared over the years, the guidelines have become more stringent

The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team

Facebook Comments