

Pig butchering scam: New cyber fraud to target youth, students, housewives

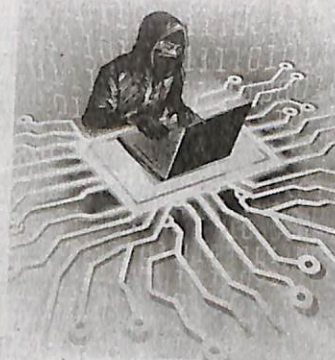
MUKESH RANJAN @ New Delhi

THE Centre has issued an alert against a new cyber fraud module called 'pig butchering scam' which has been targeting unemployed youth, students and those desperate for money, often forcing them into cyber slavery, officials said on Wednesday.

This module was also flagged in the latest annual report published by the Union Ministry of Home Affairs (MHA) last month, they said, adding, unscrupulous entities are using Google services platforms to initiate these crimes.

"According to reports from the cyber intelligence wing, a new online fraud module known as 'Pig Butchering Scam' or 'Investment Scam' has been noticed doing rounds in the cyber space, which target unemployed youths, housewives, students and needy people, who are made to either lose large sums of money daily or enticed to do cyber slavery," a senior official said.

He further said Google advertisement platform provides a convenient facility for posting targeted advertisement from across the border.



As per officials, the 'Pig Butchering Scam' is a global phenomenon that involves large-scale money laundering and even cyber slavery.

According to sources, it is believed the fraud first originated in China back in 2016. Miscreants target gullible individuals with whom they first build trust over time and then convince them to invest in cryptocurrencies or some other lucrative scheme, stealing the money collected. Officials said, the analogy to pig butchering is derived from the fattening of swine before their slaughter.

In this mode of cyber fraud, cybercriminals, after acquiring

TO FATTEN BEFORE SLAUGHTER

- Believed to have originated in China in 2016, the scam involves building trust with victim over time before convincing them to 'invest'

- **Cyber Slavery:** Victims are often enticed of coerced into becoming a partner or aide in crime

- Cybercriminals create hyperlinks on big tech and social media platforms like Google, Facebook, others

- I4C under MHA has tied up with Google, others to share threat intelligence for urgent action periodically

the trust of victim individuals, also bring them on board and engages them in different kinds of online crime as slaves.

Officials said once the trend came to light, the Indian Cyber Crime Coordination Centre (I4C) under the MHA has partnered with Google to share the threat intelligence for urgent action periodically to effectively deal with the menace.

Besides Google, cybercriminals are also using sponsored Facebook links to launch illegal lending applications in India, officials said, adding that such links are being proactively identified and flagged for necessary action.