Media Title : Daily Express
Headline : Syndicates now operating on industrial' level, say experts
Date : 29 December 2025
Section : Local
Page : 4

Syndicates now operating on 'industrial' level, say experts

PETALING JAYA: Scam activities targeting Malaysians have evolved into an industrial-scale operation powered by automation rather than being carried out by individuals, say cybersecurity experts.

Certified fraud examiner Raymon Ram said the sheer scale of scam calls and text messages blocked by authorities indicates that the operation involves robo-diallers, scripted call flows and bulk messaging systems, like a production line.

"As such, when attempts run into the billions, even a tiny success rate makes the economics work, which makes scams highly lucrative.

"It also reflects a shift in Malaysia's defensive measures with telcos and regulators increasingly stopping threats at the network level before they reach users.

"While this has prevented large-scale harm, it also shows Malaysia is a high-value target for regional scam ecosystems," he said.

Raymon said while network-level blocking is essential to counter high-volume abuse, it is insufficient.

He added syndicates adapt quickly across social media platforms and messaging channels.

"What we also need is a layered model with stronger upstream controls, faster disruption and takedowns, consistent enforcement against facilitators and victim-centric rapid response.

"The National Scam Response Centre model matters here because speed in freezing funds, stopping escalation and swift coordination between agencies is what reduces harm after prevention fails," he said.

He said a large number of scam calls originate from overseas and use voice-over-internet-protocol technology that allows calls to be generated cheaply before making its way here through international gateways.

Raymon said this makes scam operations scalable and adaptable, enabling rapid rotation of numbers and routes when blocks are imposed.

He pointed out a newer risk is voice harvesting where voice clips can be captured and potentially be used for artificial intelligence (AI)-enabled impersonation attempts.

"AI is accelerating the evolution of scams, enabling more polished and localised messages. These realistic voice impersonation create fear among potential victims who need to be constantly vigilant," Raymon said.

On Friday, the Communications Ministry revealed in Dewan Negara that since January 2022, telecommunication providers had intercepted a staggering 2.3 billion suspected scam calls and 2.5 billion unsolicited SMS messages.

Authorities also terminated nearly 187,000 mobile and fixed lines identified as sources of suspicious messaging activity.

Cybersecurity expert Fong Choong Fook said while there have been fears of "voice harvesting" by scammers through brief and silent phone calls, it was not as simple as uttering one or two words by call recipients.

"This claim made by certain parties has caused undue worry and paranoia among the public.

"It takes at least 10 to 15 seconds of recorded speech for AI to construct a credible imitation. A brief 'hello' cannot be used to generate a full conversation," he said.

Fong warned that scam activities are showing no sign of slowing down and is expected to grow even more sophisticated.

He said the public should be vigilant while authorities must stay a step ahead with enforcement and preventive measures to minimise cases of scams.

Veteran criminologist Datuk Dr P. Sundramoorthy said AI has added a professional edge to scams by generating context-aware messages mimicking banks, law firms or government agencies while voice-cloning technology lets scammers simulate authoritative or familiar voices.

He said AI-driven data analysis also enables highly personalised attacks using leaked or purchased personal data.

"Automated systems can test thousands of variations, rapidly learning which wording, timing and emotional cues elicit the highest response rates.

"The result is a shift from crude mass attempts to psychologically-tailored scams, making detection harder and scam attacks far more convincing," Sundramoorthy said.

He said recent reports of scammers impersonating law firms with claims of being able to recover funds lost to scams is a way to exploit victims' vulnerability.

"At this stage, victims are often less guarded as the desire for closure overrides caution. Scammers take advantage of this vulnerability with a false offer to recoup losses," he added.

Sundramoorthy advised the public to watch for unsolicited calls demanding immediate action, transfers, one-time passwords, unfamiliar applications or threats framed as legal or regulatory consequences.

He said even if messages appear professional or from legitimate authorities or banks, it does not require instant compliance.

"Take note that when urgency replaces verification, it is almost always a scam," he said.

The Communications Ministry also revealed that many of the phone scams rely on caller ID spoofing where fraudsters mask their true identity to display trusted or recognisable numbers.

Scammers then use psychological tactics to trick victims into revealing personal or confidential information.