NEW STRAITS TIMES

Prioritise comprehensive online safety measures over DNS redirection, says expert

By Qistina Sallehuddin - September 8, 2024 @ 6:06pm

The government should prioritise a more comprehensive approach to online safety rather than mandating internet service providers (ISPs) to implement public domain name service (DNS) redirection. - NSTP file pic

KUALA LUMPUR: The government should prioritise a more comprehensive approach to online safety rather than mandating internet service providers (ISPs) to implement public domain name service (DNS) redirection.

Universiti Sains Malaysia's cybersecurity expert Associate Professor Dr Selvakumar Manickam said implementing and maintaining a DNS redirection system would incur higher costs due to the significant investment required in infrastructure and technical expertise.

"Maintaining a DNS blocking and redirection system is a complex and costly task, demanding substantial investment in infrastructure and technical expertise.

"It can lead to a high rate of false positives, unintentionally blocking legitimate and safe websites.

"Similarly, the long-term impact on website owners could be severe, leading to potential business losses and reputational damage, despite the government's assurances that such websites would be 'quarantined' (temporarily blocked)," he said when contacted by the New Straits Times today.

DNS is a system that translates website addresses into numeric IP addresses to locate websites on the Internet.

ISPs generally operate their own DNS servers, which can be configured to block access to specific websites or domains based on their content and this method is commonly used to protect users from harmful content.

Recently, the Malaysian Communications and Multimedia Commission (MCMC) announced plans to collaborate with service providers on several preventive measures, including DNS management, to ensure restrictions on harmful or prohibited websites remain in place.

However, these measures faced criticism, with some labelling them as 'draconian'.

In response, Communications Minister Fahmi Fadzil said today that the MCMC had been instructed to halt the implementation, which was initially set to apply to businesses, enterprises, and governments by the end of this month.

The decision, Fahmi said, was made after considering public feedback through engagement sessions held by the MCMC.

Selvakumar said public concerns stemmed from fears that such measures could give the government greater control over Internet access, potentially limiting access to information and impacting freedom of speech.

"Redirecting DNS traffic to local servers raises privacy concerns, as ISPs could gain increased visibility into users' browsing habits and online activities," he added.

Instead of focusing solely on blocking public and open DNS services, he suggested that the government adopt a more comprehensive approach to online safety.

"This could include expanding educational programmes on digital literacy and parental guidance, launching public awareness campaigns, implementing age-verification and content filtering systems, strengthening cybercrime laws, collaborating with technology companies, and supporting community initiatives like hotlines and reporting mechanisms.

"(And) it is encouraging to see the government making progress in some of these areas, and further investment in these initiatives could yield long-term benefits for all Malaysians," he said.