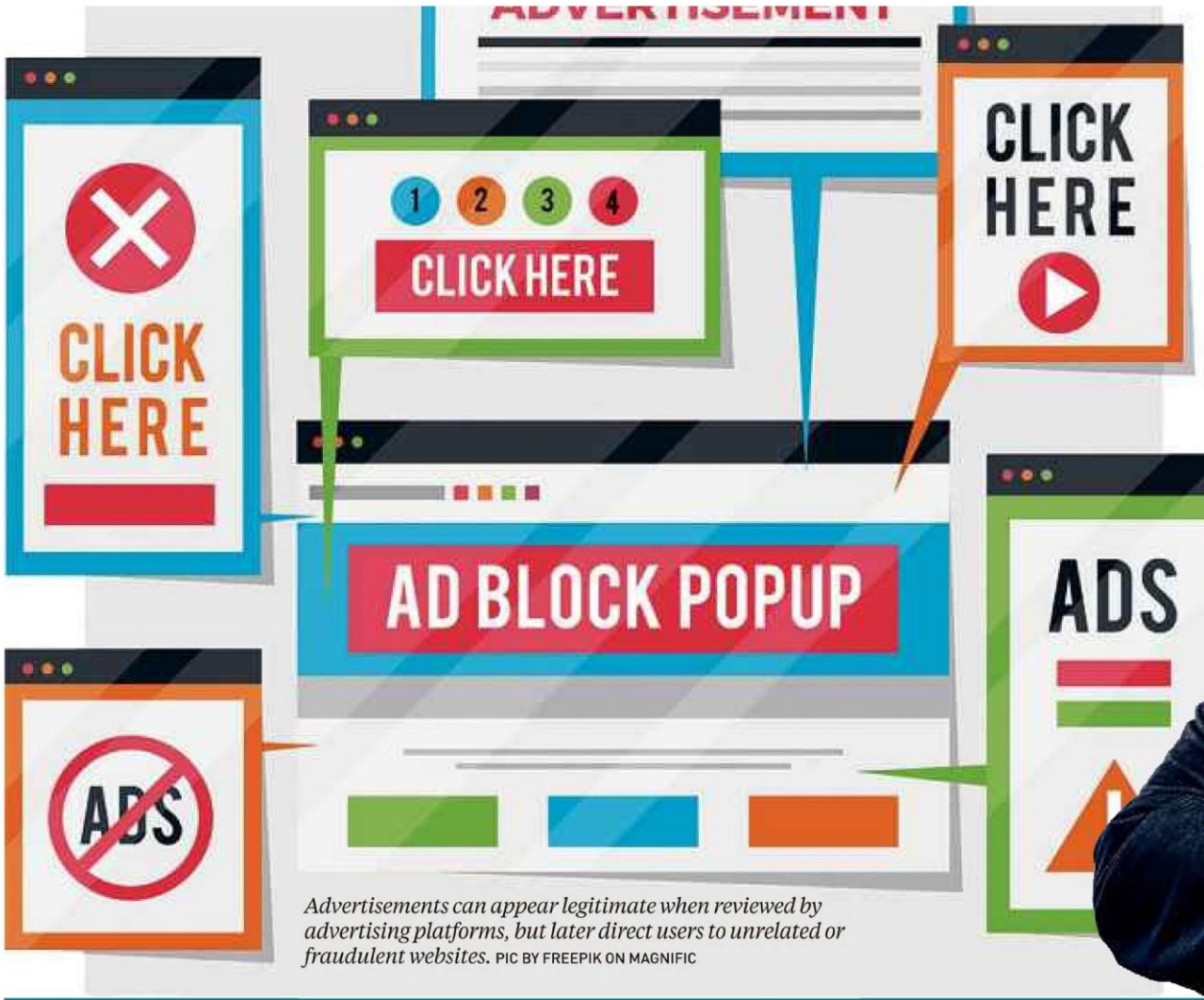
Media Title : New Straits Times
Headline : Scams cloaked by ads
Date : 24 June 2026
Section : LIFE & TIMES
Page : 13



Advertisements can appear legitimate when reviewed by advertising platforms, but later direct users to unrelated or fraudulent websites. PIC BY FREEPIK ON MAGNIFIC

Kaspersky Asia-Pacific managing director Adrian Hia

Scams cloaked by ads

INTERNET users have been warned to be wary against "ad cloaking", a scam technique cybersecurity experts say is designed to deceive users while evading online security checks.

Kaspersky Asia-Pacific managing director Adrian Hia said an ad was cloaked when it displayed different content depending on who was viewing it.

He said advertisements could appear legitimate when reviewed by advertising platforms, but later direct users to an unrelated or fraudulent website once clicked.

"It exploits users' trust in a platform, brand or service.

"Users may believe they are interacting with a legitimate website when they are actually being redirected to a fraudulent site designed to steal personal information, distribute malware or promote scams," he said.

MIMICKING TRUSTED BRANDS

Hia said cybercriminals commonly used ad cloaking to direct users to fake websites impersonating legitimate businesses, financial services, investment platforms and well-known brands.

He said these websites were designed to appear authentic, often replicating branding, layout and messaging to reduce suspicion among victims.

Once users engaged with the pages, they were frequently asked to submit sensitive personal and financial information.

"Users may be persuaded to provide personal information, banking credentials and credit card details or make payments for products and services that do not exist.

"Others may unknowingly download browser extensions, software or applications that collect data or compromise device security," he said.

Hia added that in many cases, victims believed they were dealing with legitimate services until financial losses or data misuse became apparent.

DIFFICULT TO DETECT

He said ad cloaking was difficult to detect because different content was shown to different audiences, depending on how cybercriminals configured the attack.

"Advertising platforms, security researchers and automated review systems may only see a harmless version of an advertisement, while ordinary users are redirected to malicious destinations," he said.

> *Many of these scams are designed to appear legitimate and exploit trust, familiarity and urgency to persuade users to take action without verifying authenticity.*
>
> Adrian Hia

He added that this mismatch delayed the detection and removal of harmful campaigns.

"Threat actors use various techniques to distinguish between legitimate users and automated review systems, allowing malicious content to remain hidden for longer periods," he said.

Hia said the scam was further reinforced by psychological manipulation tactics.

"Many of these scams are designed to appear legitimate and exploit trust, familiarity and urgency to persuade users to take action without verifying authenticity," he said.

He added that such tactics often caused users to act without properly checking the legitimacy of websites or offers.

HOW TO STAY SAFE

"If users suspect they have been redirected to a suspicious website, they should leave the page immediately and avoid entering any personal, financial or account information," he said.

He added that users who had shared information should act quickly to minimise potential damage.

"If information has been submitted, users should change affected passwords, enable multi-factor authentication where available and monitor financial accounts for unusual activity," he said.

Hia added that users should run a full security scan using trusted cybersecurity tools to detect malware, spyware or unwanted applications that may have been installed without their consent.

"Users should verify the legitimacy of any platform before making payments, downloading software or sharing sensitive information," he said.

For investment-related services, he advised users to confirm whether platforms were authorised by the Securities Commission Malaysia through its official Investment Checker.

"While ad cloaking is highly technical, its objective is straightforward — to trick users into surrendering sensitive information, installing malicious software or losing money," he said.

He added that the growing sophistication of such scams highlighted the need for greater user awareness, as cybercriminals continued to exploit trust in digital advertising ecosystems to reach victims.