Media Title : The Sun
Headline : Scammers prey on festive gifting
Date : 9 February 2026
Section : LYFE
Page : 24

Scammers prey on festive gifting

Beware of QR codes, payment links in circulated messages

AS Malaysians prepare for Chinese New Year and Hari Raya Aidilfitri, increased reliance on e-payments, QR codes and digital wallets has created opportunities for cybercriminals to hide scams in plain sight, with online threats remaining in the millions during the first quarter for two consecutive years.

According to data from the Kaspersky Security Network, more than 4 million web threat incidents were detected in Malaysia from January to March 2025 alone. Cybersecurity experts note that festive payment habits, including the routine use of digital transfers and QR transactions, may leave users less attentive to potential scam risks.

Bank Negara Malaysia data showed that e-payment activity averaged 409 transactions per capita in 2024. The momentum continued in 2025 with e-money values reaching RM21.5 billion in May, up more than 70% year-on-year based on industry data. As digital payments become the default for everyday transactions, users increasingly act with speed and familiarity, particularly during festive periods linked to gifting and higher spending.

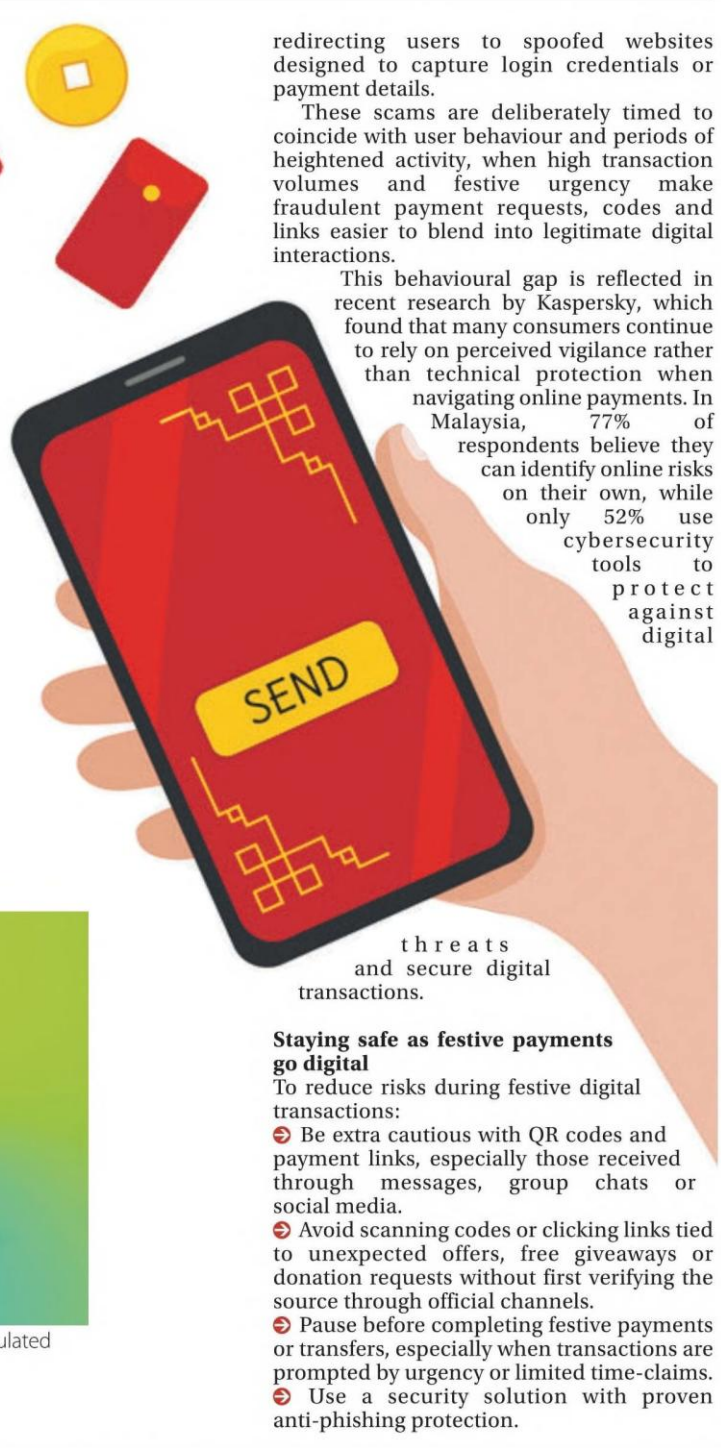
Across festive spending cycles, common payment-related scam tactics often take on seasonal disguises. Fraudulent QR codes and payment links are frequently circulated through festive-themed messages, including promotional vouchers, limited-time offers, complimentary giveaways or donation appeals shared via messaging apps and social platforms, redirecting users to spoofed websites designed to capture login credentials or payment details.

These scams are deliberately timed to coincide with user behaviour and periods of heightened activity, when high transaction volumes and festive urgency make fraudulent payment requests, codes and links easier to blend into legitimate digital interactions.

This behavioural gap is reflected in recent research by Kaspersky, which found that many consumers continue to rely on perceived vigilance rather than technical protection when navigating online payments. In Malaysia, 77% of respondents believe they can identify online risks on their own, while only 52% use cybersecurity tools to protect against digital threats and secure digital transactions.

Festive payment habits may leave users less attentive to potential scam risks. – ***123RFPIC***

Fraudulent QR codes are frequently circulated through festive-themed messages.



Staying safe as festive payments go digital

To reduce risks during festive digital transactions:

- Be extra cautious with QR codes and payment links, especially those received through messages, group chats or social media.
- Avoid scanning codes or clicking links tied to unexpected offers, free giveaways or donation requests without first verifying the source through official channels.
- Pause before completing festive payments or transfers, especially when transactions are prompted by urgency or limited time-claims.
- Use a security solution with proven anti-phishing protection.