

Media Title : The Star  
Headline : Steer clear if it's cheap and too good a deal  
Date : 21 January 2024  
Section : Nation  
Page : 3



# Steer clear if it's cheap and too good a deal

**PETALING JAYA:** There is a notable increase in ecommerce scams during festive seasons, says Raymon Ram, a criminologist who specialises in financial forensics and fraud risk management.

Scammers exploit the increased online shopping activity associated with festive occasions by creating fake online storefronts on popular ecommerce platforms or using social media to advertise their fraudulent businesses, he said.

"They lure customers with attractive deals on sought-after festive items, which are often priced lower than the market rate. Another tactic they use is the 'get it quick or lose the deal' offer," he said.

Yet another type of scam worth noting during the festive season is the scammers insisting on up-front payment through non-secure payment methods; once the deal is done, they provide fake shipping details or cut off communications with their victims.

Raymon said scammers have become increasingly sophisticated, with scammers using information available online to make their impersonations more believable.

"In Malaysia, there has been an uptick in reports of phishing scams, particularly around festive seasons. The Commercial Crime Investigation Department (CCID) and other cybersecurity experts have consistently warned the public about these scams, indicating a need for greater awareness and vigilance," Raymon said.

"There are scammers who use impersonation or phishing scams during festive seasons, often to exploit cultural practices and traditions. They impersonate friends or relatives, leveraging the custom of, for example, giving and receiving red packets or monetary gifts during Chinese New Year.

"They might send messages or email requesting financial help or

personal information, masquerading as someone the victim trusts," he said.

He advised the public to shop only on verified platforms, examine new online sellers, fact check with SemakMule.ccid to verify sellers' information such as contact details and bank account, and to stay updated.

Alliance for a Safe Community chairman Tan Sri Lee Lam Thye agrees that shoppers should be wary of new online sellers, especially those offering attractive promotions.

"It is also important to remember that, when shopping online, you should not give away any personal details that can be used by scammers.

"The public should know that depositing money into an unknown account is already suspicious, so we need to be extra cautious and use the right platforms to purchase anything for the festive season," he said.

Lee also encouraged scam victims to come forward and share their stories.

"When scam victims share their stories, it will help the relevant authorities to monitor these illegal activities and warn the public," he said.

If a deal seems too good to be true, it probably is, said MCA Public Services and Complaints Department head Datuk Seri Michael Chong, whose department often receives reports from victims of scammers who used various tactics including offering extremely cheap offers and demanding upfront payments, especially during festive seasons.

Chong said scammers use various tactics, but they often conduct their activities online.

"They use social media platforms such as Facebook and they have become very smart about luring their victims.

"Normally, people will fall for the cheap prices they offer," Chong said.

## Protect yourself when shopping online

**Step 1** Research the Seller

Before purchasing from an online seller, especially new or unknown ones, research their profile. Look for reviews, ratings, and how long they have been active. Scammers often create new profiles to sell counterfeit or non-existent products.

**Step 2** Beware of Too-Good-To-Be-True Deals

Exercise caution when you encounter deals that seem too good to be true, like significant discounts. Scammers often lure victims with attractive deals on high-demand items, especially during festivals.

**Step 3** Verify Website Security

Ensure the website is secure by checking for 'https' in the URL and a padlock symbol in the browser. Secure websites encrypt your data, reducing the risk of data theft.

**Step 4** Use Secure Payment Methods

Opt for secure payment methods like credit cards or payment services with buyer protection. These payment methods often offer protection against fraud and the ability to dispute charges in case of a scam.

**Step 5** Avoid Sharing Personal Information

Be cautious about sharing personal and financial information, especially on unverified websites or to unsolicited inquiries. Scammers can use personal information to steal your identity or access your bank accounts.

**Step 6** Use Verification Tools

Use tools like SemakMule.ccid in Malaysia to check the legitimacy of bank accounts or phone numbers. These tools help identify if an account is associated with known scams, providing an extra layer of security.

**Step 7** Regularly Monitor Bank Statements

Keep a regular check on your bank statements, especially after making online transactions. Monitoring your bank statements can help in quickly identifying and reporting unauthorised transactions.

**Step 8** Educate Yourself About Common Scams

Stay informed about common scamming tactics, especially those prevalent during festive seasons. Awareness is key to prevention, knowing the latest scamming tactics can help you stay one step ahead of scammers.

The Stargraphics