Media Title : The Star
Headline : Don't bite the scammers' bait
Date : 28 May 2025
Section : Nation
Page : 6

Don't bite the scammers' bait

Malicious links passing off as govt aid the new scourge

PETALING JAYA: Staying alert and cautious about potentially deceptive online links is not just a matter of good practice; it is an essential defence against cunning scammers who aim to drain the bank accounts of unsuspecting victims.

Recently, scammers have exploited various forms of monetary and welfare aid offered online by the government, particularly targeting the lower-income group by masking hyperlinks to deceive applicants.

Certified fraud examiner and anti-money laundering specialist Raymon Ram (*pic*) advises that being cautious of suspicious online links can help reduce the risk of online scams.

He said that in addition to emails, malicious links are now appearing across various channels, including short message services (SMS), WhatsApp or Telegram applications, social media posts and pop-up windows.

These links frequently disguise themselves as coming from reputable sources, including government agencies, banks and various service providers.

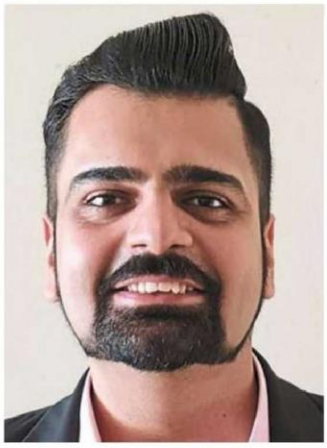
"Scammers have become skilled at making their links appear legitimate, but there are several red flags online users could look out for," he said.

He said scammers often create websites that mimic real organisations by adding small typos or extra words to genuine website addresses to hoodwink their potential victims.

Raymon said users should check the core or root domain that comes before the top domain, like "dot com", "dot gov", or "dot my", to make sure it matches the real one they want to use.

"Users should be aware that the Hypertext Transfer Protocol Secure protocol (HTTPS) does not assure safety, and neither does the padlock icon, as scammers can easily obtain these certificates.

"HTTPS alone does not prove a site's legitimacy, as it simply means the data sent is encrypted," said the founder and managing principal of Graymatter Forensic Advisory, a company that specialises in financial forensics.



He said scammers also insert messages that appear urgent or may emotionally trigger users to react and proceed without caution.

"Examples of such messages include phrases like 'your account will be suspended' or 'claim your prize now'.

"Other indicators of potential scams are poor grammar, misspellings and generic greetings.

"Also, in contrast, legitimate organisations typically address individuals by their names and maintain a professional and formal tone.

"Users are also advised to preview or scrutinise links to ascertain their destinations before clicking on them.

"If users are unsure, it's best to avoid such links and verify their authenticity with the institution they are trying to reach," Raymon said.

Asked whether a single click on a scam link can result in the loss of someone's bank account, he clarified that it typically requires multiple actions for users to lose their funds.

Raymon said there are three main pathways that lead to online theft, namely through phishing websites – where a user clicks a link and lands on a fake bank login page before providing their username, password and one-time code.

Scammers eventually use the details to access the real account and transfer money, he added.

He said another tactic is to embed malicious mobile applications such as APK files.

"A user clicks on a link that tells them to install an unofficial Android app.

"The app takes over the device and reads SMS messages, intercepts OTPs, or puts up fake banking screens to get login information.

"These programmes allow scammers to watch the user's activities and capture sensitive information.

"Hence, it is not the first click itself that empties a bank account but a chain of actions that occurred earlier," he said.

He said scammers also hide dangerous links to trick people, which is a common method used in phishing and other scams.

"Scammers may hide links in several different ways.

"One example would be putting up a button or text that says 'Visit Bank Negara', but a hidden link that takes people to a different website," Raymon said.