



Digital wedding invitations among latest scam tactics

Public warned against downloading APK files that scammers can use to access personal data and financial details

BY QIRANA NABILLA MOHD RASHIDI
newsdesk@thesundaily.com

PETALING JAYA: The public has been warned not to blindly download wedding invitations sent to their phones as they could lose their life savings.

Commercial Crime Investigation Division director Datuk Seri Ramli Mohamed Yousuf said wedding invitations are among the latest tactics used by scammers since mid-2023.

"They email wedding invitations embedded with Android Package Kit (APK) files and when a recipient downloads them, scammers can obtain access to their financial details and steal their data.

"APK is a file format used by Android to distribute its apps. It contains the required components for installation for the phones to work.

"But scammers are embedding APK files with malware in the guise of digital wedding invitations. So, before downloading files, check if the link contains an APK extension."

He said apps should not be downloaded from messages or emails but only from secure platforms such as Google Play and the Apple App Store.

"If people install APK files from unknown sources or scammers pretending to be family members or friends, criminals could gain access to the phone without the victim's



Ramli said police require the cooperation of those who have been victimised to step forward and lodge reports for effective monitoring and analyses. – ADIB RAWI YAHYA/ THE SUN

knowledge, which is how bank accounts are cleaned out."

He said in 2023, there were 676 scam cases with losses of RM18,561,092.25.

As of May, there were 67 similar cases with losses of RM1,105,590.55. Selangor and Penang reported the highest numbers.

Ramli said phone hacking is a common criminal tactic to gain unauthorised access to an individual's data and financial information.

"The tactic is not new and initially involved job offers, cleaning services, maid agencies and the sale and purchase of vehicles. Now, scammers are using digital wedding invitations.

"If someone is unaware of APKs and scam tactics, they might believe the invitation is from a friend and download the file. This could result in them losing their life savings."

He said when downloaded, APK

files activate a process that extracts data from the victim's contact list and scammers who access personal data could engage in identity theft and other methods to transfer funds and conduct various illicit activities.

"Unless encryption technology akin to that employed by banks is used, unsuspecting individuals are likely to provide opportunities for scammers to steal data."

He said while police monitor scam tactics, they require the cooperation of those who have been victimised to step forward and lodge reports for effective monitoring and analyses.

He added that this would help police to share information with relevant agencies, such as the Malaysian Communications and Multimedia Commission to prevent such incidents.

"Investigations are challenging as the phone numbers used by

scammers are linked to malware, making it difficult to trace their origins.

"It is crucial for victims to report such incidents so that we can analyse and collaborate effectively to combat cybercrime."

Ramli said individuals must check the file extension before downloading or responding to emails, even if they are from supposed contacts within their circle.

He also said addressing the challenges presented by scammers requires a concerted effort by all parties, including enforcement agencies and the public.

"Scam victims should immediately call 997, which is our National Scam Response Centre. We could try to block fund transfers if we are notified as soon as possible. Victims should also file a police report to facilitate a formal investigation."