PermataBank

BEWARE!
Online Fraud Mode Under the Guise of .APK Files

The "Fake .APK File" scam is increasingly widespread and creative. Usually, it is sent via Whatsapp under the guise of delivery/courier info, wedding/seminar invitations, BPJS invoices, SatuSehat Mobile download links, credit card bills, and many other forms.

Be cautious! If you click on the .APK file, it will automatically steal your personal data, from contact info, SMS content to banking info such as the OTP Response Code.

How Does It Work?

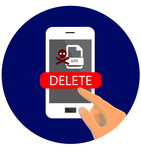
1. The fraudster sends an .APK file to make potential victims curious and click on it.

2. After the potential victim installs the application and allows access to the .APK file, data from the device will be stolen.

How to Avoid .APK File Scams?

1. Never click or download .APK files received from strangers posing as package courier or bank employees, even under the pretext of sending the wrong messages/news. Ignore and delete the .APK files immediately.

2. Make sure the news or documents you receive are the things that you planned and needed, rather than being delivered unexpectedly.



3. Ignore any instructions to open the contents of the message in the .APK file or download and install the .APK file. Your mobile device will be infected by malware (malicious software) that can potentially steal your personal data and financial information.

4. Verify the source of the application to be installed comes from the official **Google Play Store** or **App Store** source.

5. Do not permit to access contact or storage on your mobile device.

If you get suspicious chats, SMS, calls, or e-Mails on behalf of **Permata**Bank, please contact contact:

Permata**Tel 1500-111** dan **021-29850611**

care@permatabank.co.id | @PermataCare

PermataBank, PermataHatiCSR

@PermataBank, @PermataHatiCSR