MEGHALAYA RURAL BANK

Cybersecurity Digest

Bi-Weekly Update by O/o CISO of Meghalaya Rural Bank

Volume 3 Issue 2

Date: 16.04.2026

APK Fraud

In recent times, there has been an increase in cases where fraudsters trick users into installing malicious APK files through calls, messages, and social media platforms. Android is a widely used mobile operating system, especially in India. While its open-source nature allows easy customisation and access to multiple apps, it also opens a window for cyberattacks. Cybercriminals may deploy malicious APK (Android Package) files that pose a threat to the security of your data. This blog will explore how fraudsters use these files, the potential risks, and the steps you can take to protect your device.

APK File

An APK File is a package file format used by the Android Operating System for distributing and installing mobile apps. An APK File, also known as an Android Package, contains all the necessary components for an app to install in your device. Think of it as the Android equivalent of an executable file (.exe) on Windows. These files contain all the elements an app needs to install on your device.

Typically, users can download APK files from Google Play Store, an official and trusted source. However, APK files can also be obtained from third-party sources, which are not guaranteed to be safe. While third-party app stores can offer legitimate apps, they also pose significant security risks.

How scammers use APK Files?

Cybercriminals use sophisticated social engineering tactics to trick users into downloading and installing malicious APK (Android Package) files. Here is a step-by-step breakdown of how they may take control over your phone device:

- **Posing as a reliable source**: Fraudsters often pose as trusted entities such as bank representatives or customer support agents on email, social media, or messaging apps. They create a sense of urgency or necessity to convince the user to download an APK file.
- **Delivery:** The user receives the APK file via email, SMS, or a direct download link. These messages are crafted to look legitimate, often mimicking official communication styles.
- **Installation**: When the user attempts to install the APK file, they are warned about the risks of installing apps from unknown sources. Additionally, the app requests extensive permissions, such as access to the camera, microphone, location, contacts, and SMS. Once installed, such malicious APKs may contain keyloggers or remote access tools that secretly capture sensitive information and transmit it to the fraudster through a command-and-control (C&C) server. This allows the attacker to monitor activities and misuse the device without the user's knowledge.
- **Execution**: If the user proceeds with the installation, the malicious app begins to actively monitor device activity and capture sensitive information such as passwords and personal messages.
- **Sending stolen information:** Once installed, the malicious app secretly sends the gathered information, like passwords and personal messages, to the scammer's computer. This gives the scammer remote access to control the device.

Consequences of APK Fraud

APK fraud can have serious consequences, including:

Malware Installation: Malicious APK files can install malware on your device, which can steal sensitive information or cause damage to your device. This malware can operate in the background, often without your knowledge.

Data Theft: Cybercriminals can use malicious APK files to steal sensitive information such as login credentials, credit card numbers, or personal data. This can lead to identity theft and significant financial losses.

Financial Loss: You may incur financial losses due to unauthorised transactions or purchases made using your stolen information. Hackers can gain access to your bank accounts and make fraudulent transactions.

Device Damage: Your device may be damaged or compromised due to malware or other malicious activities. This can result in reduced performance, frequent crashes, or even complete device failure.

Reputation Damage: If your device is used to spread malware or engage in other malicious activities, your reputation may be damaged. This is particularly concerning for public figures or individuals in sensitive professions.

By understanding the risks associated with APK fraud and following the precautionary measures outlined in this article, you can protect your device and personal information from potential threats.

Precautionary Measures

To protect your device from APK File Fraud, follow these essential steps:

Avoid Unsecured Networks: Do not use unsecured Wi-Fi or public networks for sensitive transactions or downloads. Hackers often exploit these networks to intercept data.

Be cautious with Third-Party Apps: Never download APK files from unknown sources, especially if prompted by an unsolicited call or message. Stick to trusted sources.

Install Antivirus Software: Use reliable antivirus software to detect and block malicious files. Regularly update the software to protect against new threats. Many antivirus apps can scan APK files before installation.

Reset your phone: If you suspect a malicious file has been installed, reset your phone to factory settings immediately. This will remove any malicious apps and restore your device to a clean state.

Reboot regularly: Restarting your phone can disrupt ongoing malware processes and reduce the risk of prolonged infection. It is a simple yet effective way to maintain your device's health.

Report suspicious activity: Immediately report any unauthorised transactions or suspicious activity to your bank. Additionally, you can report cybercrime to the National Cyber Crime Reporting Portal at **cybercrime.gov.in** or call their helpline on 1930. Additionally, you can file a complaint with the Cyber Crime Cell through the **SacharSathi Portal**, which offers case tracking.

Verify if the message is official: Be extra careful when you get messages or calls on your mobile number claiming to be from the bank's WhatsApp number. Verify the message by contacting the bank directly using their official contact details.

Scan your device for malware: Download and run the eScan Bot Removal Tool (version 7.2.0.59) available on Google Play Store. This tool is part of the Cyber Swachhta Kendra initiative by CERT-In,designed to help users detect and remove malware or bot infections from their mobile devices.