

E-Challan Scams

This is a new cyber fraud where scammers pose as traffic authority and make people download a fake app for paying challans. This app is actually malware that steals sensitive information from mobile like SMS, banking apps, OTP and passwords.

In this scam, cyber criminals pose as traffic police or government agency officials and send fake challan messages through WhatsApp, SMS or email.

It states that your vehicle has violated traffic rules and you need to pay a fine. Along with this, an APK file (like e-parivahan.apk) or link is provided, which claims to install this app to view challan details or make payment.

When the user downloads this file and installs the app, it requests access to sensitive information from the phone such as SMS, contacts, banking apps, passwords



and OTPs. Once this access is granted, scammers steal money from accounts through mobile banking or UPI.

How to differentiate between real and fake e-challan messages?

Real challan messages come from government's official SMS IDs (like VK-MORTH, CH-TRAFF etc.) and do not mention any APK files or suspicious links. For genuine challan

information, you need to visit government websites like <https://echallan.parivahan.gov.in> and enter RC number or driving license number. Whereas fake challan

messages contain fear-inducing language and pressure to download APK files or click on links.

What to do if you have downloaded a fake app?

- Uninstall the app immediately.
- Go to mobile settings and remove all permissions.
- Change passwords for your bank, UPI and social media accounts.
- If money has been withdrawn or you are being blackmailed, file a complaint at the nearest cyber crime cell.
- Additionally, you can file an online complaint on the cyber crime portal.

The official mParivahan app is only available on Google Play Store or Apple App Store. Its developer is 'NIC eGov Mobile Apps'. Additionally, you can verify its official link by visiting <https://parivahan.gov.in>.

What precautions should be taken to avoid such fake apps ?

Scammers take advantage of fear and urgency to make users make mistakes. You can protect yourself from such fraud by following the measures given below.

- Never install any app from an APK file.
- Do not click on any link provided in the challan

message.

When you receive a challan message, first check it on the official government website.

Before downloading any app, check the app developer's details and ratings on the playstore.

Always verify the URL

carefully before clicking on any link.

Keep your banking SMS and UPI apps secured with an app lock.

If in doubt, verify on the official website of the traffic police.

Can antivirus or security apps stop such fake apps?

Some mobile security apps do scan APK files and give warnings, but they don't guarantee 100% security. The best approach is to download apps only from Google Play Store or Apple App Store. Also, never install APK files received through messages or websites.



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS



Indian
Cyber
Crime
Coordination
Centre





E- CHALLAN SCAM

Your Challan No is 3489157841xxxx for xx08xx8182 having total challan amount as Rs. 500. For online payment of challan visit:

<https://echallanparivahan.in/>

you can also contact RTO office for disposal of challan.
Regards,
RTO

FAKE LINK

ORIGINAL LINK
<https://echallan.parivahan.gov.in/>



If you receive a link for traffic challan, don't click these links.
As clicking upon these links for payment, fraudsters can hack your bank account.



FOR ANY CYBER CRIME COMPLAINT REPORT TO: <https://cybercrime.gov.in>

In case of online financial fraud DIAL 1930



FOLLOW US ON:

