THE TIMES OF INDIA

This WhatsApp message from traffic department may be 'dangerous'

Hackers exploit WhatsApp to spread malware by sending deceptive messages posing as authorities to steal personal information. Quick Heal warns against downloading unfamiliar apps and granting permissions to prevent sensitive data theft. To stay safe, users must be cautious of unexpected messages and avoid downloading unfamiliar apps.

Hackers have devised a new way to target people and this time, they are utilising the WhatsApp messaging system of the government's traffic department to spread their malicious software, a report has said. According to a report by Quick Heal, hackers are spreading malware on Android phones through fake WhatsApp messages which appear to be from the government, "but they're hiding something nasty inside."

The cybersecurity company claims to have encountered several instances of deceptive messages purportedly sent from authorities like the Pimpri-Chinchwad Traffic Police and Chandigarh Traffic Police.

While these messages look harmless, they contain a malicious link that downloads a malicious software on the users' devices and steal their personal information

The message claims that the recipient has received a ticket for breaking traffic rules. To make the messages seem authentic, the hackers include specific details such as the ticket number and the vehicle's registration information.

Additionally, the sender also uses official logos of the Maharashtra Motor Vehicle Department and Chandigarh Administration as their profile pictures to further establish authenticity. These messages request the receivers to download an application called

“Vahan Parivahan.” Unknown of the potential danger, the receiver of that WhatsApp message downloads a malicious file that is designed to steal sensitive information from Android devices.

The malicious app also initiates a request for various permissions, including the ability to send and receive SMS messages, manage phone calls and access the device’s contact list. It also seeks authorisation to be the default SMS application, thereby, assuming control over messaging functionalities.

Once the malware application gets permission, it hides its icon and secretly starts gathering sensitive information from the device.

To stay safe, users must be cautious of unexpected messages and avoid downloading unfamiliar apps.