The Russian company F6 in its Telegram channel warned Rossyan that attackers who are trying to hack Android-scartphones often use trojan programs that allow them to remove the device remotely. These Troyans are masked for real applications of banks, payment systems, delivery services and other services.

Experts said that one of the ways use scammers is a modification of the NFCGATE program designed to improve the work of the NFC chip, which is needed to pay using a smartphone instead of a card. According to experts, scammers persuade a person to install a malicious application on the phone, pretending him for something useful. After that, they gain access to the NFC function, payment system and banking cards of the victim.

Attackers also actively use ads on the search for remote workers. They send to potential victims links to sites that look like a Google Play app store. On these fake resources, it is proposed to download a malicious application, which then steals bank cards, messages and notifications.

Another common method is reward surveys. Fraudsters, as a rule, on behalf of a large organization offer people to participate in a paid survey. To do this, they ask to download the malicious application to the phone, which then requests access to messages and contacts.

F6 explained that to protect the phone from malicious programs, the operating system and applications should be regularly updated. Moreover, it is critical where to download the programs from: it is necessary to download all applications only from official sources, such as the Russian Rustore store. This store checks the developers and applications in order to prevent the program with outdated safety rules or too much advertising to its platform.

In addition, users need to be careful with incoming messages: do not open suspicious investments and links in e -mail and instant messengers. The installation of reliable antivirus is also important.