In early May, news of hacking through WhatsApp garnered headlines after the revelation of a mobile phone spyware - a malicious software used to infiltrate the device and steal the data causing a threat to the security of the users. The security breach enabled the sophisticated cyber actors to install the bug into the targeted user’s phone just by making a missed voice call (an unattended call) which will not even be visible in the phone’s log thereby leaving no traces behind. The spyware would let the hackers trawl the messages, texts, calls or other information on the devices of the target users.

WhatsApp, a Facebook-owned-messaging App is considered simple and safe and is used by approximately 1.5 billion users all over the world, sending more than 65 billion messages per day. The issue affected WhatsApp for Android prior to v2.19.134, WhatsApp Business for Android prior to v2.19.44, WhatsApp for iOS prior to v2.19.51, WhatsApp Business for iOS prior to v2.19.51, WhatsApp for Windows Phone prior to...
Often users are not aware of the importance of updating the software for operating systems or Apps. Installing the updated software is important to secure your device against vulnerabilities.

- Set strong and difficult passwords for every service or App and keep changing the password regularly.

If possible, enable two-factor authentication/verification to restrict hackers signing into the accounts which may reduce the risk of unsecured passwords or shared passwords being hacked from different sites you use.

Install/download secure and trustworthy apps or services which give malware security. Refrain from downloading fake or pirated software and stop clicking on unknown links in emails or messages which may download malicious programmes on the device.

Keep deleting the browser history and clean the memory of your device regularly because the web browsers like Chrome, Firefox keep records of the sites visited for some time which may enable attackers to steal the details of online activities.

Avoid using free unsecured wireless access on public networks for financial transactions as this is an open invitation to hackers.

Public WiFi VPN (Virtual Private Network — private server for remote areas) protection can be installed so that the data travelling between devices (computer and mobile) and the VPN server is securely encrypted.

Use the secure version of standard “Hypertext Transfer Protocol (HTTP)” i.e. HTTPS. Here, ‘S’ stands for ‘Secure’. HTTPS (Hypertext Transfer Protocol Secure) is used for secure communication over networks. A lock icon in the address bar can also be clicked to know more about website security.

There are certain basic network settings which could be manually adjusted in the device like trusted and non-trusted networks, etc.